

# **RISK MANAGEMENT POLICY AND FRAMEWORK**

**Bound and Beyond Public Company Limited**

Reviewed and effective since November 22, 2023

## **RISK MANAGEMENT POLICY**

---

Bound and Beyond Public Company Limited (“the Company”) has realized that the Company has faced the various risks and uncertainties in conducting its business. Therefore, the Company is committed to the management of risk in conjunction with strategic management to ensure that corporate growth is aligned with corporate objectives and goals with an acceptable risk appetite.

The basic principle of Corporate Risk Management is that the Company runs business to add value to the stakeholders while the business runs under uncertainty and challenge. The corporate risk management is considered to assist the Management to overcome the uncertainty and various risk effectively and efficiently. It also identifies opportunities to add value to the organization, meets the expectations of stakeholders, promotes sustainable business operation, and complies with the good corporate governance principles.

Risk Management Policy and Framework was implemented to ensure that there is a risk management system throughout the Company and its subsidiaries efficiently and effectively. The Policy has prescribed as follow;

1. The Risk Management Committee was appointed by the Company’s Board of Directors, and the Company’s Managing Director shall serve as member, by position. The Risk Management Committee is responsible for scrutinizing, recommending, and monitoring to ensure that risks are effectively managed in accordance with the scope of duties prescribed in the Risk Management Committee Charter.
2. To define an enterprise – wide management system and process in accordance with international standard to manage the risks faced across the entire organization.
3. To set protective guidelines and risk mitigation measures for the Company’s activities and business, to reduce potential damage or loss including impact from possible risks and contribute to the achievement of defined goals of the organization.
4. To implement the risk reporting systems to inform the risk management to the Company’s Management, the Risk Management Committee, the Audit Committee and the Board of Directors about the information on key risks, trends and overall risks as well as oversee the risk effectively and efficiently.
5. To determine risk management framework to ensure that the Company can work according to its risk management approach, and is able to identify and forecast risks with potential negative impacts to the Company’s operation and goals in every aspect. Similarly, the Company has developed plans to continuously control, monitor, and improve risks through management, control and review mechanisms. These components ensure that risk level is under the risk appetite level.
6. To determine an embedding corporate-wide risk management culture. Such arrangement promotes understanding, raises awareness and engagement for all level of employees on the topic of corporate-wide risk management.
7. This Policy and Framework shall be reviewed and assessed at least once a year to ensure that those are consistent with current business’s conditions of the Company.

This Risk Management Policy and Framework was reviewed, improve and came into effect since November 22, 2023 onwards.

## RISK MANAGEMENT FRAMEWORK

---

### **Section 1: Background**

The Board of Directors is aware of and highly appreciates the importance of the risk management. Therefore, the Risk Management Committee has been set up, consisting of Independent Directors served as the Chairman of the committee, Director, the Managing Directors and employees who understand the Company’s operation, to jointly manage risks at both the corporate and the business unit level and to supervise the management of corporate risks thoughtfully and thoroughly. The Risk Management Committee has established the foundation for risk management by applying corporate risk management elements in accordance with the standard of “The Committee of Sponsoring Organizations of the Treadway Commission: COSO”, Operational Framework, and Risk Management Procedures in accordance with “Risk Management – Principles and Guidelines” to management of risk to be under an appropriate or acceptable level to achieve the objectives, strategy, vision and mission set by the Board of Directors.

This Risk Management Policy and Framework consists of content on the definition of risk management elements, risk management practices, risk management structures, responsibilities according to risk management structure, risk management framework and process, and business continuity management, to be used by the risk management entity as a management approach, which is a tool that helps all business units of the Company to achieve objectives/goals and operational success, leading to the creation of added value and sustainable growth of the organization.

### **Section 2: Definition**

- Risk** : The uncertain events that may occur in the future, if they occur, will have a negative effect on the achievement of an organization’s objectives, missions, or operation opportunities, or cause it to lose business opportunities.
- Identifying risk** : The consideration of what event will hinder the achievement of objectives, the Company’s missions, operation opportunities, or business opportunities.
- Risk Factor** : The original cause or source of risks, and events that will lead to not achieve in the objectives and goals set. In each factor, the true causes of the factors are determined. It can be explained that the risk factor’s cause results in any risk, and measures can be implemented to manage the factors in order to reduce the risk of occurrence.
- Risk assessment** : The measurement of the risk’s severity in order to prioritize it based on its likelihood and impact.
- Likelihood** : The possibility or frequency which a risk event will occur.
- Impact** : The severity of the damage or the consequences of a risk event.
- Risk level** : The level of risk derived from assessing the likelihood and impact of each risk factor, divided into five (5) levels; very high, high, medium, low, and very low.

- Source of risk** : It is occurred from a consequence of two factors: internal and external.
- Internal factors include organization’s objectives, policies and strategies, operation, work process, structure and management system, finance, corporate culture and information technology.
  - External factors include government policies, economic conditions, social, political conditions, the actions of relevant external entities, competition, vendors or service providers and natural disasters, etc.
- Risk management** : The management of factors and controlling activities that may cause risk to operational processes by reducing the source of the risk and decreasing the potential adverse consequence of uncertainty to a tolerable level. The Company can be assessed, controlled, and monitored systematically by taking into account the accomplishment of its objectives or goals or maximizing the Company’s value under business uncertainty. After risk assessment, the evaluator selects the most appropriate risk management method.

**Section 3: Key elements in risk management**

The effective and efficient risk management in accordance with the COSO guidelines consists of eight components that cover the following guidelines for policy-establishment, operation and risk management criteria:

1. **Internal Environment:** The organizational environment is a key component in defining the risk management framework, and it is an important basis for determining the direction of the organization’s risk management framework. It consists of various components, such as organizational culture, management policies, personnel practices, work procedures, an information system, etc.
2. **Objective Setting:** To clearly and appropriately determine the organization’s risk management goals, the organization must consider formulating risk management objectives in line with the strategic goals and risks acceptable to the organization.
3. **Risk Identification:** It is a collection of events that may occur with the business units, including both internal and external risk factors. When they occur, the organization’s objectives or goals are not achieved. In order to understand the events and circumstances, the Company evaluates the risk factors that may occur with personnel management policies, operations, finances, the information system, regulations, and so on. In addition, the Management can consider implementing guidelines and policies to cope effectively with the potential risks.
4. **Risk Assessment:** Risk assessment measures the degree of severity of a risk to determine its prioritization by assessing its likelihood and impact.

5. **Risk Response:** This is conducted once the organization has identified the risk and assessed the risk level. Response measures must be implemented in order to minimize the possibility of the risk occurring or the severity of the impact to an acceptable level for the organization. It is worthwhile to invest in the most appropriate risk management approach.
6. **Control Activities:** identifying activities and procedures to assist in mitigating or controlling risks in order to ensure that they are appropriately managed, and enabling operations to fulfill corporate objectives and goals, including preventing and minimizing risk to an acceptable level.
7. **Information and Communication:** An organization must have a functional information and communication system, as it serves as an important foundation for further considering risk management in accordance with the frameworks and procedures stipulated by the organization.
8. **Monitoring:** A follow-up is required for the organization to determine whether performance is appropriate and risks can be effectively managed.

The Company has adopted COSO-EERM 2017 (Enterprise Risk Management - Integrating with Strategy and Performance), which divides the enterprise risk management process elements into five components in order to achieve the sustainable development goals of the business.

1. Corporate Governance and Culture
2. The Company's strategy and objective setting
3. The Company's performance goals
4. The review and revision
5. Information, Communication and Reporting

#### **Section 4: Type of Risk**

The risk type has been classified as follows:

1. **Strategic Risk (S):** refers to the risk resulting from improper strategic planning and compliance, including inconsistencies between policies, goals, strategic plans, organizational structure, competing circumstances, resources, and environment that affect the Company's objectives or goals.
2. **Operational Risk (O):** refers to the risk resulting from each step of the operation as a result of a lack of good governance or a lack of adequate internal control. It covers processes, equipment, information technology, operational personnel, and the property safety factor.
3. **Financial Risk (F):** refers to the risks related to financial liquidity, financial management, and financial statements, such as risk from improper budgeting, mis-budgeting, and overhead, including risks from fluctuations in market factors (market risk) and risks from counterparties failing to fulfill obligations (credit risk), as well as the risk of fluctuations in interest rates and exchange rates.

4. **Legal /Compliance Risk (L):** refers to the requirement for the Company's business units to comply with the law and corporate obligations, such as the risk of breach of contract, obligation, lack of compliance reporting, or non-compliance with laws, rules, and regulations.
- 5 **Emerging Risk (EM):** refers to losses arising from risks that are not present but may occur in the next 3 – 5 years later due to changing environmental conditions. These types of risks are slowly occurring that are not easy to identify. There is a low frequency of occurrence, but they may have a severe impact once they occur. These emerging risks are often identified based on projections under existing studies. These emerging risks are often the result of political, legal, social, technological, physical environments, natural changes, or pandemics. Sometimes the effects of these types of risks may not be currently identifiable. For example, problems arising from nanotechnology, climate change, the risk of spreading serious infectious diseases, and so on.
6. **Fraud/Corruption Risk (C):** refers to the risk of fraud, corruption, embezzlement, solicitation, or transfer of an organization or external entity's interest for personal gain.
7. **Environmental Risk (EN):** refers to the risk that negatively impacts the environment caused by the Company's operation, such as climate change resulting from the product design or service, material procurement, water scarcity, the production process or service, increased costs from taxing industries or businesses that emit carbon dioxide (Carbon Tax), and so on.
8. **Social Risk (SO):** refers to the risk that negatively impacts the environment caused by the Company's operations, such as human rights violations in the supply chain, the change of people's behaviors, the inability to create innovation to respond to consumer behavior so that the organization is unable to create the value that responds to the goals, and so on.
9. **IT Risk (IT):** refers to
  - Digital Transformation Risk means the risk that the Company will be unable to adapt to the technological changes that may impair corporate operations, causing it to lose competitiveness.
  - Cyberthreat risk means being attacked by an external intruder who destroys or damages a network or database in an organization's information technology system.
10. **Business Interruption Risk (BI):** refers to the Company's temporary suspension to repair or correct property damage caused by cyberattacks, information technology, natural disasters, political rallies, epidemics, and other changes that cause business to cease, and so on.

#### **Section 5: the Company's Risk Management**

The Company presently has various aspects of risk management through the use of several management tools, such as Good Corporate Governance and Key Performance Indicators (KPIs). In practice, the Company has been able to effectively control operational risk by implementing a quality policy in accordance with numerous standards. Nonetheless, the Board of Directors has placed great emphasis on risk management in order to ensure effective and efficient risk management. The Board of Directors has therefore appointed the Risk Management Committee to oversee risk management more effectively.

**1. Risk Management Structure**

Those responsible for the Company’s risk management consist of employees at all level, from the general officer to the Board of Directors level. The structure is as follows:



**2. Role of those involved in risk management**

Based on the Risk Management Structure, the roles and responsibilities of each Department are defined role and responsibilities as follows:

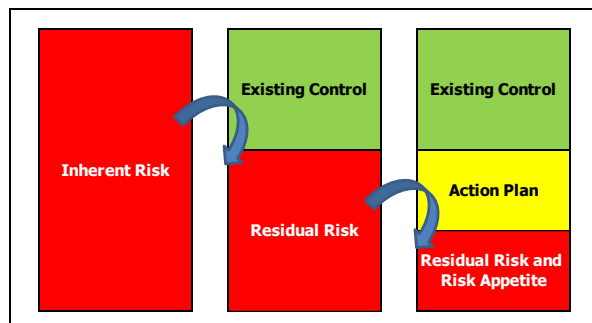
Department	Role and Responsibilities
<p><b>The Board of Directors</b></p>	<ul style="list-style-type: none"> <li>- To supervise the Risk Management Committee in order to ensure effective risk management throughout the organization through the Risk Management Committee.</li> </ul>
<p><b>The Risk Management Committee</b></p>	<ul style="list-style-type: none"> <li>- To consider and propose the Risk Management Committee Charter and the Risk Management Policy and Framework to the Board of Directors for approval.</li> <li>- To consider the risk assessment criteria and risk response plan in order to cope with the key risks in line with the risk appetite level and report the risk assessment result and action plan to the Board of Directors.</li> <li>- To supervise the Management’s regular risk analysis, assessment, and management.</li> <li>- To review the risk management report in order to ensure that the organization has adequate and effective risk management systems in place.</li> <li>- To ensure that the secretary of the committee is responsible for coordinating and reviewing that the Company has an appropriate risk management system in place to identify risk, assess risk, and create action plans for risk mitigation that are in line with the risk appetite level.</li> <li>- To arrange the Risk Management Committee’s meeting at least once per quarter to monitor the Company’s risk status and the progress of risk management, including following up on what needs to be improved to be in compliance with the Risk Management Framework.</li> <li>- To supervise and motivate employees at all levels to be aware of risk and encourage an ongoing enterprise-wide risk management process into organizational culture.</li> <li>- To prepare a risk management report for inclusion in the Company’s Annual Report.</li> </ul>

<p><b>The Risk Management Working Team</b></p>	<ul style="list-style-type: none"> <li>- To identify risks, implement risk management methods, evaluate, and monitor each business unit's risk management.</li> <li>- To analyze and assess risks in accordance with the risk assessment criteria and the risk management framework.</li> <li>- To compile a summary and report on the risk assessment results and action plan for presentation to the Risk Management Committee.</li> <li>- To develop the risk management framework and persuade all business units to implement it efficiently.</li> <li>- To encourage employees to continuously acquire knowledge on risk management.</li> </ul>
<p><b>Head of Business Units</b></p>	<ul style="list-style-type: none"> <li>- To analyze and assess the risks of each function and report the risk to the Risk Management Working Team.</li> <li>- To regularly study, analyze and report potential risks to the Risk Management Working Team.</li> <li>- To report to the Risk Management Working Team on the status of performance in accordance with the action plan.</li> </ul>
<p><b>General Officer</b></p>	<ul style="list-style-type: none"> <li>- To implement an internal control system to prevent risks. Any operations that are deemed to be at risk or are likely to be at risk must be regularly reported to the supervisor.</li> <li>- To carry out risk management in accordance with established guidelines.</li> </ul>

**Section 6: The Company's Risk Management Principles**

Risk is the possibility that an event will occur and impact the Company's ability to achieve its objectives, such as increased competition, corruption, non-compliance, and so on. The fundamental principle in risk management is to assist the Company in creating value by incorporating a risk management perspective into all phases of normal operations and any business decisions. Risk factors must definitely be considered. There are guidelines for adaptability and operating under uncertain conditions. It is appropriate for the Company and the current circumstances. Personnel factors, participation, transparency, and corporate culture must all be considered for the best possible foundation. Most importantly, it must be constantly applied and reviewed on a regular basis.

**Risk Management Concept**





**Section 7: The Company’s Risk Management System Framework**

The Company has adopted the following risk management system framework in accordance with the COSO guidelines.

**1. Identifying incidents**

The managers or department heads must identify potential risks affecting both internal and external factors, as well as risk-related issues. To enhance risk management, all stakeholders must be transparent and open in identifying risks that affect the execution of strategies or the achievement of objectives or events.

**2. Risk Assessment**

Risk assessment is a process that consists of analyzing, assessing, and categorizing risks that affect the achievement of the Company’s operational objectives. The Company has developed criteria for assessing various risks, including the likelihood and severity of the impact, which can be determined using both quantitative and qualitative criteria. These criteria serve as the foundation for assessing various risks. Referring to **Appendix B**, the risk assessment must take into consideration both the inherent risk and the residual risk, including emerging risks, which can be defined as both quantitative and qualitative criteria as a basis for assessing risks.

Furthermore, the fraud or corruption risk assessment is developed to identify, assess, and review the fraud and corruption risks, as well as to raise awareness of the corruption risks that affect the Company’s objectives and operations. To ensure that anti-corruption measures are stipulated in accordance with the assessed risks, the risk assessment must be in conformity with the Company’s corruption policy framework.

**3. Risk Rating**

To assess the risk, a “Risk Profile” is defined to assess the risk based on the risk significance rating from the likelihood and impact as well as the extent of the acceptable risk level (the risk appetite boundary) based on **Appendix A**.

Level of risk = (likelihood of occurrence of events) X (impact of events)

**4. Risk Treatment**

The employees directly involved in the risk management process are responsible for risk management. The establishment of a risk management strategy will be presented to the management committee meeting, which will assess and approve the allocation of resources required to carry out the activity (if any). By selecting the most appropriate risk management strategy, the acceptable risk (Risk Tolerance) will be taken into account, with the resulting cost compared to the benefits. This includes legal and other requirements related to social responsibility. Choose the strategy for risk management as follows:

- **Risk avoidance (Terminate)** is the decision to avoid risk due to its high impact and likelihood, such that another operational process is chosen to keep the Company from encountering the risk event while still achieving the original target performance. For example, the project divestment and business model reform, and so on.
- **Risk Transfer (Transfer)** is the process of minimizing the likelihood or impact of risk by transferring responsibility to another individual or other entity to carry out risky activities on behalf of the group without limiting the risk only to the extent that the risk is the responsibility of other operators. Purchasing insurance, outsourcing, engaging in hedging activities, and so forth are examples.
- **Risk control (Treat)** is to implement additional risk control activities to ensure that the risk status is mitigated sufficiently. This could mean minimizing the likelihood of a risky event or the severity of its consequences.
- **Risk acceptance (Take)** occurs when the benefits and returns from a risk activity outweigh the cost of personnel, budget, and resources invested in that risk activity. The Company will allow that risky activity by strengthening risk controls to minimize the risk level as low as practicable.

#### **5. Control Activities**

The management operation policies and procedures that have been developed to assure that the risk has been effectively managed through control activities such as preventive control, detective control, and corrective control.

#### **6. Monitoring and Review**

The Company shall review its risk management policy on a regular basis, whether annually or when significant changes and impacts on risk management occur because a change in environmental conditions results in improper or inefficient control activities and the inability to achieve the Company's objectives. As a result, the risk management monitoring process should be established appropriately at each level.

#### **7. Information and communication technology**

The Company has noted the importance of enterprise risk management. It has been established that the Company's risk management policy is communicated to its employees by publishing it on the Company's intranet, through training, or workshop to ensure that all employees acknowledge and understand the risk management process as well as their roles and responsibilities.

Furthermore, the Company makes its risk management policy and framework available on its website so that all stakeholders are informed of the Company's risk management information.

#### **Section 8. Limitation**

Although the Company's risk management is very valuable, a successful risk management approach can also have limitations. Limitations can arise as a result of the discretion and erroneous decision-making required to respond to risks. Furthermore, the costs and benefits must be considered, as well as the factors that are out of the Company's control.

**APPENDIX**

**A. Risk Consideration Level**

**1 Risk Appetite: the acceptable risk level → Very Low, Low and Medium**

<b>Likelihood → Impact ↓</b>	<b>Unlikely (1)</b>	<b>Moderate (2)</b>	<b>Possible (3)</b>	<b>Likely (4)</b>	<b>Almost certain (5)</b>
<b>Very High (5)</b>	<b>High</b>	<b>High</b>	<b>Very High</b>	<b>Very High</b>	<b>Very High</b>
<b>High (4)</b>	<b>Medium</b>	<b>High</b>	<b>High</b>	<b>Very High</b>	<b>Very High</b>
<b>Medium (3)</b>	<b>Low</b>	<b>Medium</b>	<b>High</b>	<b>High</b>	<b>Very High</b>
<b>Low (2)</b>	<b>Low</b>	<b>Low</b>	<b>Medium</b>	<b>High</b>	<b>Very High</b>
<b>Insignificant (1)</b>	<b>Very Low</b>	<b>Low</b>	<b>Medium</b>	<b>High</b>	<b>High</b>

<b>Risk Level</b>	<b>Risk Management Measures</b>
<b>Very High</b>	“Unacceptable” the business units have to establish action plans urgently and immediately in order to remain acceptable.
<b>High</b>	“Unacceptable” the business units have to establish action plans immediately in order to remain acceptable.
<b>Medium</b>	“Acceptable” but at the “high level”, business units must concentrate their attention on risk assessment and develop action plans if it deems necessary. It also has to endeavor to reduce the risk so that it remains acceptable.
<b>Low</b>	“Acceptable” The business units do not need to adopt new procedures for risk management but must strictly adhere to the existing internal control system. Ensure that there is constant and controlled monitoring to prevent it from reaching an unacceptable level.
<b>Very Low</b>	“Acceptable” the business units do not require to develop the new measure of risk management.

(-Translated Version-)

■ **The risk likelihood level is set at five levels.**

Likelihood	Level	Probability/Opportunity
Very High	5	A much worse chance of transition if there is no supporting activity.
High	4	A worse chance of transition if there is no supporting activity.
Medium	3	Opportunity for change is low despite supporting activities or taking no action.
Low	2	Opportunities for change are better, but they need to be promoted.
Very Low	1	Opportunities for continuous change in a better way without taking any action.

■ **The severity level of the impact is set at five levels.**

Impact	Level	Effects/Consequences
Very High	5	Very high impact, uncontrollable.
High	4	High impact but controllable (difficulty).
Medium	3	Has a moderate but controllable effect.
Low	2	It has little impact and is easily controllable.
Very Low	1	It has very little or no direct impact.

**B. Risk Assessment Criteria**

■ **Impact and Likelihood:**

1. **Impact Factor – Revenue or profit:** determined by the amount of the revenue or profit deficit generated.

Very Low (1)	Low (2)	Medium (3)	High (4)	Very High (5)
< 3% of the financial target	>3 - 5% of the financial target	>5 - 10% of the financial target	>10 - 20% of the financial target	> 20% of the financial target

Insignificant (1)	Unlikely (2)	Moderate (3)	Possible (4)	Likely (5)
< 10% or once per 5 years	10 - 25% or once per 2 - 4 years	26 - 50% or once per 1 - 2 years	51 - 75% or once per 2 - 6 months but no more than 5 times	> 75% or once a month or more

(-Translated Version-)

**2. Impact Factor – cost or expenditure:** by the increased cost or expense:

Very Low (1)	Low (2)	Medium (3)	High (4)	Very High (5)
< 3 - 5% of costs/expense	> 3 - 5% of costs/expense	>5 - 10% of costs/expense	>10 - 20% of costs/expense	> 20% of costs/expense

Insignificant (1)	Unlikely (2)	Moderate (3)	Possible (4)	Likely (5)
< 10% or once per 5 years	10 - 25% or once per 2 - 4 years	26 - 50% or once per 1 - 2 years	51 - 75% or once per 2 - 6 months but no more than 5 times	> 75% or once a month or more

**3. Impact Factor – Customer Satisfaction:** determined by the number of complaints received:

Very Low (1)	Low (2)	Medium (3)	High (4)	Very High (5)
< 5 times per year	> 5 - 10 times per year	>10 - 20 times per year	> 20 - 30 times per year	> 30 times per year

Insignificant (1)	Unlikely (2)	Moderate (3)	Possible (4)	Likely (5)
<10%	11 - 25%	26 - 50%	51 - 75%	> 75%

**4. Impact Factor –the Company’s image and reputation:** determined by extent of damage or impact on the stakeholder:

<b>Very Low (1)</b>	<ul style="list-style-type: none"> <li>Risks that are always common in the ordinary course of business.</li> </ul>
<b>Low (2)</b>	<ul style="list-style-type: none"> <li>Impact in organization or employee level.</li> <li>Minor damage to the company’s image and reputation.</li> </ul>
<b>Medium (3)</b>	<ul style="list-style-type: none"> <li>Impact on customers.</li> <li>Moderate damage to the company’s image and reputation.</li> </ul>
<b>High (4)</b>	<ul style="list-style-type: none"> <li>Impact on shareholders, investors, financial institutions and analysts.</li> <li>Damage that affects the image and reputation of the company a lot.</li> </ul>
<b>Very High (5)</b>	<ul style="list-style-type: none"> <li>Impact on trading partners, local communities, local public sector and public agencies.</li> <li>Massive damage to the company’s image and reputation.</li> </ul>

Insignificant (1)	Unlikely (2)	Moderate (3)	Possible (4)	Likely (5)
< 10% or once per 5 years	10 - 25% or once per 2 - 4 years	26 - 50% or once per 1 - 2 years	51 - 75% or once per 2 - 6 months but no more than 5 times	> 75% or once a month or more

**5. Impact Factor – Environment, Health, Safety and Community:** determined by the adverse effects to environment, health, safety, and community derived from the operation:

Very Low (1)	Low (2)	Medium (3)	High (4)	Very High (5)
<ul style="list-style-type: none"> <li>Leak of little hazardous substances.</li> <li>Leak of hazardous substances in-house.</li> </ul>	<ul style="list-style-type: none"> <li>Leak of hazardous substances in-house.</li> <li>Spend little time to deal with problem.</li> <li>No patients.</li> </ul>	<ul style="list-style-type: none"> <li>Leak of hazardous substances in-house.</li> <li>Spend time to deal with problem.</li> <li>Found patients.</li> <li>Minor injured.</li> </ul>	<ul style="list-style-type: none"> <li>Contamination of hazardous substances to adjacent area.</li> <li>Be able to deal with problem but need more time.</li> <li>Found patients.</li> <li>Medium injured.</li> </ul>	<ul style="list-style-type: none"> <li>Contamination of hazardous substances to adjacent area.</li> <li>Fail to deal with problem promptly.</li> <li>Found patients.</li> <li>Seriously injured or death toll.</li> </ul>

Insignificant (1)	Unlikely (2)	Moderate (3)	Possible (4)	Likely (5)
< 10% or once per 5 years	10 - 25% or once per 2 - 4 years	26 - 50% or once per 1 - 2 years	51 - 75% or once per 2 - 6 months but no more than 5 times	> 75% or once a month or more

**6. Impact factor – Fraud and Corruption**

- The risk impact level is set at five levels.

Impact	Image/Reputation Aspect	Financial Aspect	Legal Aspect	Customer Aspect
<b>Very Low (1)</b>	Negative news from the local media was dealt with quickly; events returned to normal.	< 5% of income.	There is minor noncompliance with regulations.	Very few customer complaints, no impact on costs.
<b>Low (2)</b>	Negative news impacts the company's products and reputation in the domestic market.	Between 5% - 10% of income.	Lawsuit, fine, or small amount of damage taken place.	Minimal impact on customer relationships, with some fixed costs.

<b>Medium (3)</b>	Negative news from the local media is still present and is beginning to affect customers.	Between 10% - 20% of income.	Significant lawsuits, including substantial fines/damages claims.	Loses or impacts relationships with customers to a large extent, with a mid-cost solution.
<b>High (4)</b>	Negative news in the national media and the Asian region will affect the company's reputation and image in the long term.	Between 20% - 30% of income.	The investigation may include criminal proceedings and/or significant claims for damages.	Significant loss or impact of relationships with key customers with substantial cost reductions and impact on future growth.
<b>Very High (5)</b>	Widespread news was presented through the media, both within the country and abroad.	> 30% of income.	Criminal investigations, claims for damages, and/or orders to suspend any transactions were carried out.	Loses a significant customer and has severe consequences for future growth.

- The risk likelihood level is set at five levels.

<b>Likelihood</b>	<b>Occurrence Quantity</b>	<b>The status of the event. Actual Occurrence.</b>	<b>Occasion commits an offense</b>
<b>Very Low (1)</b>	The chance of occurrence is < 10% or once per 5 years.	Incidents have been reported and are currently under investigation.	Happens very quickly without control measures.
<b>Low (2)</b>	10 - 25% chance of occurrence or once per 2 - 4 years.	Incidents under management.	There is a greater chance of accidents without control measures.
<b>Medium (3)</b>	26 - 50% chance of occurrence or once per 1 - 2 years.	The incident was handled.	There is a chance that this will happen without control measures.
<b>High (4)</b>	51 - 75% chance of occurrence or Once per 2 - 6 months, but no more than five times.	Incidents under management.	There is a greater chance of accidents without control measures.
<b>Very High (5)</b>	The chance of occurrence is greater than 75%; or One time per month or more.	Incidents have been reported and are currently under investigation.	Happens very quickly without control measures.

**C : RISK ACTION PLANS TEMPLATE:**

<b>Risk Management Plan</b>	
<b>Risk Ref. No.</b>	
<b>Key Risk</b>	
<b>Business Function/site</b>	
<b>Risk Level</b>	
<b>Risk Treatment Plan</b>	
<b>1. Detailed action plan</b>	
<b>2. Resource requirements</b>	
<b>3. Responsible person</b>	
<b>4. Timeframe / Milestone</b>	
<b>5. KPI / KRI</b>	
<b>6. Reporting/ Monitoring</b>	



(-Translated Version-)

**D. Risk Profiles:**

**Business Function/Site .....**

**Objectives : .....**

Ref No.	Key Risk	Risk Category	Existing Control	Risk Level		Action Plan	Risk Owner
				Impact	Likelihood		
1.							
2.							
3.							
4.							
5.							