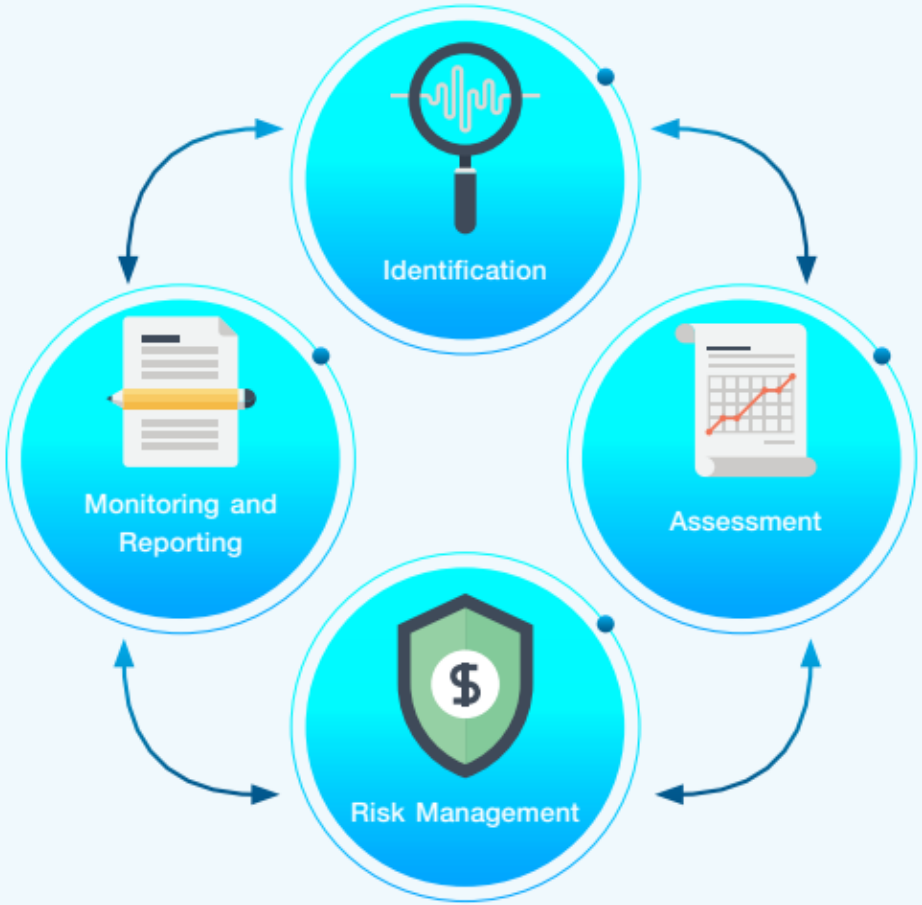
# Risk Management

January 31, 2023

RISK MANAGEMENT
Retention
Immunization
Systems
Knowledge

# 1. Risk Management Processes




Risk management process on yearly basis consist of 4 steps as follows;

1. Risk Identification
2. Risk Assessment
3. Risk Treatment and Mitigation
4. Monitoring and Reporting

For Company's risk management process, risk identification is carried out to assess risks caused by factors that will continuously affect the organization. PTG considers risks based on both internal and external contexts, needs and expectations of stakeholders, relevant laws or regulations, and formulates a concrete risk management plan that covers the entire organization. It aims to reduce the level of various risks to meet the risk appetite of the organization and to build confidence among stakeholders by demonstrating that the Company can continue its business under changes that may occur, including monitoring and reporting on the results of enterprise risk management and department-level risks. All of the information shall be reported to the Enterprise Risk Management Working Group and the Risk Management Committee to continuously monitor risk management and sustainably achieve both short- and long-term objectives, as well as goals, of the organization

# 1.1 Description of risk appetite or risk tolerance levels for at least two risk categories/ types

| Risk Categories | Risk Appetite |
|---|---|
| **Strategic Risk** | The company has a process for determining corporate strategies that are consistent with the vision and company goals. The company considers risks in putting strategies into appropriate practice, to be able to manage risks that may affect operations according to corporate strategy and reduce damages that may result from strategic risks and drive the company's performance to effectively achieve the goals set. |
| **Financial Risk** | The company has managed risks that may affect financial performance, keep it at a level acceptable to the company and consistent with the company's financial goals, finding new business opportunities. Business operations are conducted with appropriate consideration of returns to stakeholders. The company has managed financial risk and investment risks so that returns on investment are as expected and the company's performance achieve a sustainable growth. |
| **Operational Risk** | The company does not accept risks that affect the operations of important transactions of the company and affecting cyber security, which may result in the company being unable to continuously run the business. The company does not accept risks that affect the safety of employees, customers and all groups of stakeholders. The company focuses on continuous business operations. It does not cause a severe impact on the company's core business. |
| **Compliance Risk** | The company focus on compliance with all relevant policies, laws, rules and regulations to make sure that its operations are accurate, reliable and transparent to all parties. The operations according to the principles of good corporate governance to promote transparent operations, anti-corruption and achieve in complying with related rules and regulations. |

The company has determined risk appetite levels for use in risk assessment and management. Any risks that have been assessed are found to be it may affect the company beyond the risk appetite levels. The company assign to the department that the risk owner prepare a risk mitigation plan.

# 1.2 Prioritization of identified risks

| Risk Map | | | Likelihood | | | | |
|---|---|---|---|---|---|---|---|
| | | | Very Low | Low | Medium | High | Very High |
| | | | 1 | 2 | 3 | 4 | 5 |
| IMPACT | Very High | 5 | 5 | 10 | 15 | 20 | 25 |
| | High | 4 | 4 | 8 | 12 | 16 | 20 |
| | Medium | 3 | 3 | 6 | 9 | 12 | 15 |
| | Low | 2 | 2 | 4 | 6 | 8 | 10 |
| | Very Low | 1 | 1 | 2 | 3 | 4 | 5 |

The company will assess the risk level in order to prioritize risks. The prioritization of risks is the basis for considering and selecting methods to respond risks. Calculating the risk level by multiplying the scores between the likelihood of occurrence and the impact in order to prioritize and use in deciding which risks should be mitigating with first.

Once the risk level of each risk has been assessed. It will be compared in the Risk Map by dividing the risk level into 4 zones:

- Red zone (Very High)
- Orange zone (High)
- Yellow zone (Medium)
- Green zone (Low)

Risks can be prioritized by managing risks in the red zone or the very high zone first. Then descend in order the risk is in the orange zone and yellow zone, respectively.

# 1.2 Prioritization of identified risks

| Risk Map | | | Likelihood | | | | |
|---|---|---|---|---|---|---|---|
| | | | Very Low | Low | Medium | High | Very High |
| | | | 1 | 2 | 3 | 4 | 5 |
| IMPACT | Very High | 5 | 5 | 10 | 15 | R1 | 25 |
| | High | 4 | 4 | 8 | R2 | 16 | 20 |
| | Medium | 3 | 3 | R2 | 9 | R1 | 15 |
| | Low | 2 | 2 | 4 | 6 | 8 | 10 |
| | Very Low | 1 | 1 | 2 | 3 | 4 | 5 |

**Example :**

When assessing the level of likelihood and impact of Risk from oil price volatility (R1), the risk level is in the red zone (Very High) and assessing the level of likelihood and impact of Cyber security risk (R2), the risk level is in the orange zone (High). When prioritizing Risk from oil price volatility should be managed ahead of Cyber security risk.

However, after the risk has been managed by a mitigation plan. The level of risk is reduced.

R1 Risk from oil price volatility (before mitigation plan)

R2 Cyber Security Risk (before mitigation plan)

R_ Risk level after mitigation plan

# 1.3 Description of mitigating actions for at least two risks identified.

## 1) Risk from oil price volatility

Various factors and situations that occurred and affect the price of crude oil in the world market, causing incessant volatility, examples of which are the world economy, political and economic stability in different countries, conflicts among major oil producers, International war, etc. These factors are beyond Company's control. The volatility of crude oil prices in the global market may directly affect the selling price of fuel, both retail and wholesale, resulting in fluctuating demand and sales volumes of fuel. Moreover, it may influence the values of inventories, which are mostly fuel, as well as having an impact on Company's financial position and performance.

## Mitigation Plans

In order to manage potential risks, the Company has measures to address risks.

- The Company monitors the oil price situation on a daily basis and presents a report regarding the oil price situation to the executives and related parties for their acknowledgment in order to manage the oil procurement and inventory to stay in the appropriate level, in line with the economic situation, crude oil price, and changing demands.
- Daily inventory management reports and information on the movement of oil prices are produced to analyze the consistency of oil stocks to ensure that they correspond to the fluctuating oil prices in order to manage oil inventory and increase the profitability of the Company.
- Tools have been developed to assist management of oil price risks.

However, in order to mitigate the risks of the Oil Business, which is subject to high volatility due to the world crude oil prices, the Company addresses the risks to lessen impacts on its business goals by investing in Non-Oil and Renewable Energy Businesses, increasing the proportion of new businesses that consistently generate income and finding ways to reduce operating costs, as well as other expenses, to maintain performance and reduce the impacts on business operations caused by the volatility of oil prices.

# 1.3 Description of mitigating actions for at least two risks identified.

## 2) Cyber Security Risk

Widespread cyber threats that will affect the data security of the Company are another factor that greatly affects the business. If a cyber threat occurs and the Company does not have a supporting measure or good management measure in place, it may cause significant damage. Besides, it may also affect corporate image, credibility, and confidence of stakeholders while there could be financial consequences after cyber threats which cause impact to the Company's capital management.

## Mitigation Plans

the Company has implemented risk management measures as follows:

- The Company formulated an IT Security Policy.
- The Company has risk management in place to reduce cyber threat impacts by providing measures to prevent cyber threats and arrange IT Security audits, as well as raising awareness of cyber threats among employees at all levels.
- The Company conducts penetration testing on its important systems to prevent cyber attacks. This is a method of assessing development risks in order to address weaknesses or detect vulnerabilities within the system. The Company carries out this assessment regularly to find risk possibilities and solve them before an actual risk occurs, as a measure to prevent cyber threats.
- The Company has an IT Disaster Recovery Plan in place whereby its IT system has been tested continuously, especially in part of cyber security, to ensure that the system can operate without interruptions due to cyber threats. The plan is reviewed regularly so that it is in line with the current situation