Risk
Management

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) Cyber Security Risk

Cybersecurity threats loom large, presenting a considerable risk to the information security of the Company. This factor profoundly affects our business operations. Without sufficient preparedness or robust management measures, cyber threats can inflict substantial harm on the organization. Moreover, such incidents can erode the Company's reputation, credibility, and trustworthiness among stakeholders. Furthermore, the financial implications of cyberattacks can disrupt our financial management.

Mitigation Plans

the Company has implemented risk management measures as follows:

- The Company maintains a robust IT Security Policy.
- It proactively mitigates cybersecurity risks by deploying diverse measures to prevent cyber incidents and bolster security protocols across all departments. Additionally, comprehensive efforts are undertaken to cultivate awareness of cybersecurity threats among employees at every hierarchical level.
- The Company regularly conducts Penetration Testing on its critical systems as a proactive measure against cyber attacks. This method involves identifying vulnerabilities and weaknesses, thus enabling the assessment of potential risks within the system. By pinpointing specific areas of vulnerability, the Company can take necessary steps to address and mitigate existing risks. Penetration Testing is an integral component of the Company's cybersecurity strategy.
- Employee awareness of cybersecurity is actively promoted through various internal communication channels within the organization.
- The Company places significant emphasis on developing and maintaining an IT Disaster Recovery Plan, with a specific focus on cyber security aspects. Continuous testing of this plan ensures that IT operations can continue seamlessly even in the event of a cyber threat or disaster. Furthermore, the plan undergoes regular review and updates to align with evolving cybersecurity threats and current organizational circumstances.

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

2) Environmental Risk

In operating the business, there may be some activities that affect the environment and contribute to global warming, e.g., CO2 emitting operations of oil depots and oil transportation vehicles, etc. The Company thus attaches great importance to mitigating environmental impacts, reducing carbon dioxide and GHG emission, minimizing energy consumption of the operations in various areas in order to manage risks that may affect the environment.

Mitigation Plans

- Implemented an integrated palm oil project to promote the use of renewable energy and support the idea of operating an environmentally-friendly business.
- Initiated projects to construct energy-efficient gas stations, incorporating solar rooftops to generate electricity for internal use. Additionally, promoting the use of clean and renewable energy while reducing electricity costs within the gas station premises.
- The Company has devised a comprehensive action plan for calculating and compiling reports on the organization's Carbon Footprint. It has received certification for the Carbon Footprint for the Organization encompassing the headquarters, oil depots, transportation fleet, and gas stations from the Thailand Greenhouse Gas Management Organization (TGO).
- The Company has been registered for the Thailand Voluntary Emission Reduction Project (T-VER) by Thailand Greenhouse Gas Management Organization (Public Organization) (TGO) in recognition of its solar rooftop project rolled out in 29 gas and LPG stations.
- Prepared a climate change risk and opportunity analysis report. It operates according to the risk management process by identifying, analyzing, and evaluating risk factors and opportunities from climate change in accordance with the principles of the Task Force on Climate-related Financial Disclosures (TCFD). Moreover, the Company has assessed risk factors and the likelihood of climate-related impacts and provided climate change risk management measures.
- The Company is engaged in a waste management business initiative aimed at harnessing electricity from renewable energy sources. This comprehensive project encompasses several key operations, including waste separation systems for producing refuse-derived fuel (RDF), waste to-energy power plants for electricity generation, and the production of compost from organic waste derived from the waste segregation process.

2. Has the risk management department been audited by an external auditor?

Risk management department has been audited to ensure its operations comply with the operating manual by Internal Audit, and its activities are monitored according to the requirements and standards of ISO9001 by the Quality System Assurance and Management Division. Additionally, it is also audited by External Auditor, PricewaterhouseCoopers Consulting (Thailand) Ltd. (PwC), which conducts regular audits of the company's risk management operations as part of the annual financial statement audit.