SD-CS-PO-10

Risk Management Policy

TAT

THAI AUTO TOOLS AND DIE PUBLIC COMPANY LIMITED

(“The Company”)

Risk Management Policy

Business operations today face rapid changes in operations due to external factors such as changes in economic conditions, politics, government policies, technology, and competition in the industrial sector, and internal factors such as changes in organizational structures. To make management more flexible and responsive to changing external factors, such as labor shortages and other issues, which directly affect the Company's operations, Thai Auto Tools and Die Public Company Limited ("**the Company**") recognizes the importance of corporate risk management and believes that corporate risk management is a process that will help reduce the monetary and non-monetary impacts that may occur from both external and internal factors. Moreover, risk management will help build confidence among investors and the company 's stakeholders.

Therefore, the Risk Management Committee has established a policy for managing risks in the Company and subsidiaries (collectively referred to as the "**Group**") as follows:

- The Risk Management Committee promotes for risk management to be the responsibility of everyone in the organization who must be aware of the risks inherent in their own departments and the organization's operations and prioritize managing various risks to ensure they are at an adequate and appropriate level, and encourages employees to understand the causes of risks and take corrective actions. This includes determining the tools to help prevent or reduce potential risks in order to achieve the objective of preventing and reducing potential losses.
- The Risk Management Committee supports the establishment of an organization's risk management process that complies with international standards and practices to ensure effective management of risks that may impact the Group's operations. This includes the development and implementation of risk management practices throughout the organization in the same direction and using the risk management system as a tool for decision-making in planning the strategies, work and operations of the Group.
- The Risk Management Committee supports the establishment of guidelines for preventing and mitigating operational risks to avoid potential damage or loss, including adequate and consistent monitoring and evaluation of risk management.
- The Risk Management Committee supports the use of information technology systems in the risk management process, as well as an effective risk management reporting system for the management, the Audit Committee and the Board of Directors.

ORIGINAL

Risk Management Framework

To ensure that risk management complies with the Company's policy, the Risk Management Committee has established a risk management framework. This framework serves as a tool to identify potential risks in each work process, to predict the severity or impact if an event occurs, and to identify ways to manage those risks to reduce them to an acceptable level or with the least impact on the Group.

Risks

Risks refer to likelihoods or situations that are uncertain or that cause current plans or operations to not achieve their set objectives or goals, ultimately leading to impact or damage to the organization, whether in terms of monetary impact or the organization's image and reputation.

Risk Management

Risk management refers to a process practiced by the Board of Directors, executives and all personnel in the organization to help determine strategies and operational procedures. The risk management process is designed to identify potential events that may have an impact on the organization, and to manage those risks to an acceptable level for the organization to have reasonable confidence in achieving the organization's stated objectives.

Enterprise Risk Management Process

The key steps in the enterprise risk management process are as follows:

1. Objectives Establishment.
2. Risk Identification.
3. Risk Assessment.
4. Risk Treatment.
5. Monitoring and Reporting.

1. Objectives Establishment

1. To enable the organization to reduce the potential for future damage to an acceptable, controllable and auditable risk level.
2. To serve as a guideline for implementing the risk management process in a systematic and continuous manner.
3. To serve as a tool for communication and creating understanding of operations within the organization to be able to link risk management with the organization's strategy.
4. To have a system for continuously monitoring and reviewing the results of risk management operations and monitoring new risks that may arise.
5. To build trust with business partners to increase the value of the organization.

2. Risk Identification

Risk identification must identify the sources, affected entities, events and their causes, as well as potential impacts.

Risk identification may be conducted by interviewing senior executives or management responsible for particular work plans or operations and compiling the key risk issues of interest or concern to compile a corporate risk profile, which refers to the types of risks that are likely to occur in the future or that could cause the organization to lose business opportunities. Risk identification should consider both the internal and external environments of the organization.

External environment refers to the various elements outside the organization that influence the organization's objectives or goals such as the following:

- Changes in culture, economy, society, consumers, environment, finance, technology, laws, regulations and standards related to the Group.
- Political stability.
- Competitive environment both in the country and abroad.
- Key drivers and trends impacting organizational objectives.
- Acceptance and value of external stakeholders.

Internal environment refers to things within an organization that influence the achievement of organizational goals such as the following:

- Organizational capabilities in terms of resources and knowledge such as capital, time, personnel, processes, systems, and technology.
- Information systems, information flow processes in both accounting and operations, and formal and informal decision-making processes.
- Internal stakeholders.
- Conflict of Interest.
- Corporate policies, objectives and strategies.
- Organizational awareness, values and culture.
- Standards and models developed by the organization.
- Structure such as management system, roles and responsibilities.

Risk Types

The Risk Management Committee has classified risks into four categories:

1. **Strategic Risks (S)**

   These risks arise from the formulation of strategic plans, operational plans and their implementation that are inappropriate or do not comply with various factors such as government policies, changes in laws and mass problems, etc.

2. **Financial Risks (F)**

   These consist of risks related to finances such as interest rate changes, exchange rate fluctuations, and counterparty risks, etc.

3. Operational Risks (O)

Operational risks are risks that every business inevitably faces. They arise from people, work processes, technology, and external factors. These risks may arise from normal business operations, including legal risks, and each business must find ways to control and manage these risks to prevent them from occurring. If a business allows operational risks to become excessive, its performance may not be as expected and could result in damage to the business.

4. Compliance Risks (C)

These risks arise from violations or non-compliance with laws, regulations or standards related to operations and include risks arising from failure to perform duties in accordance with the policies and procedures established by the organization.

3. Risk Assessment

Risk assessment is a step that must be taken after risk identification. Risk assessment consists of two main processes as follows:

3.1 Risk Analysis

This process is the consideration of the causes and sources of risks as well as the consequences that follow, whether positive or negative, including the possibility of the consequences that may follow. The factors that create impacts and the likelihood of their occurrence must be identified. Furthermore, an event or situation may have consequences and affect the objectives or goals in many aspects. Therefore, risk analysis should include consideration of the risk management measures currently in place or implemented, as well as their effectiveness.

3.2 Risk Assessment

Risk assessment is a comparison of risk levels obtained from analysis by comparing risks with the risk appetite. In cases where a risk level is not within the risk appetite, the risk must be managed immediately.

Risk Criteria Specification

The criteria used in assessing risks should reflect the values, objectives and resources of the organization. Some criteria may be developed based on legal requirements, regulatory requirements, member organizations or the potential for loss of revenue if an event occurs. The criteria must be consistent with the organization's risk policy and reviewed on an ongoing basis.

Current Characteristics Used to Determine the Risk Criteria

- The nature and types of impacts that can occur and approaches to impact assessment.
- Guidelines for identifying likelihood of occurrence.
- Timeframe of likelihood and impacts.
- Guidelines for determining risk levels.
- Risk appetite.
- Risk level requiring management.

Likelihood/Impacts of Risk Events

The likelihood of a risk event occurring and its impact are divided into five levels defined as follows:

Level	Likelihood
5	Very high
4	High
3	Medium
2	Low
1	Very Low

Levels of Impact Affecting:

reputation / image / credibility / share prices / financials / competitiveness / production and operational capability are divided as follows:

Level	Impact
5	Severe impact / Production disruption / Halt of operation
4	Significant impact
3	Medium impact
2	Very low impact / controllable
1	No impact on the Company

The severity of the risks can be divided into 5 levels as follows:

5	Red	=	Very high severity level, immediate action required.
4	Pink	=	Severity level is quite high, action is required.
3	Dark yellow	=	Medium to high severity level, action required.
2	Light yellow	=	Medium severity level, regular monitoring required.
1	Green	=	Low severity level.

The Risk Management Committee shall consider and set the severity criteria for risks as a guideline for implementation.

Figure 1 Risk Assessment Table

Severity of Impact	Likelihood				
	1 – Very Rare	2 - Rare	3 - Occasional	4 – Frequent	5 – Regular Occurrence
5 - Very Severe					E = Very High
4 - Severe				H = High	
3 - Medium			MH = Medium-high		
2 - Low		M = Medium			
1 - Very Low	L = Low				

Once assessment has been completed, the Risk Management Committee may appoint a risk management sub-committee to assist in operations as follows:

- Analyze and summarize the assessment results by using the risk map above and prioritizing risk topics.
- Present assessment results to the Executive Committee meeting to select key risk topics that require management and designate the part of management that is in charge (risk champion) to implement additional risk management measures in addition to those currently in place.
- Present risk issues and measures that need to be managed further to the Risk Management Committee, Audit Committee and the Board of Directors for acknowledgement.

4. Risk Treatment

The Risk Management Committee may appoint a working group to assist in the preparation of a risk management plan, which will be presented to the Board of Directors for consideration and approval of the allocation of necessary resources (if any). In selecting the most appropriate risk management approach, consideration must be given to the risk tolerance, the costs incurred compared to the benefits to be gained, and other relevant laws and regulations.

In deciding on a risk management approach, consideration should be given to risks that, if left unaddressed, may not make economic sense, such as risks that have a significant adverse impact but are highly unlikely to occur. Risk management approaches may be considered on a case-by-case basis or may be implemented concurrently with other risks.

Risk Management Guideline

1) Avoid means avoiding/canceling activities that create risks. This approach is often used when the risks are so severe that it is impossible to reduce or manage them to an acceptable level.
2) Retain is an approach for controlling potential risks to their current level when the risks are too costly to justify the benefits.
3) Reduce means the provision of management measures to reduce the likelihood of risk events occurring or to mitigate their potential impact, such as by preparing a contingency plan.

4) Exploit means making use of risks while taking into account competitiveness.

5) Transfer is the transfer of all or part of risks to a party/agency outside the organization to help bear or limit the risk instead, such as by purchasing an insurance policy or hiring an expert.

5. Monitoring and Reporting

The Risk Management Unit or the working group appointed by the Risk Management Committee will coordinate with the management in charge of risks to report on the statuses of risks, including the risk management process, to executive meetings, the Risk Management Committee, the Audit Committee and the Board of Directors for acknowledgement or further consideration.

Management should analyze and monitor changes in the internal and external environments, including changes in potential risks, which may result in a review of risk management and prioritization, and these may be used to review the overall risk management framework.

This policy was approved by the Board of Directors Meeting No. 4/2025 on 14 November 2025, effective from 14 November 2025 onwards.

- Dr. Damri Sukhotanang -
Dr. Damri Sukhotanang
Chairman of the Board of Directors