Risk Management Policy

Srisawad Corporation Public Company Limited

Index

1. Introduction

This Enterprise Risk Management Policy has been established as a framework and guideline for risk management operations of the Srisawad Group. This policy serves as a tool to support personnel in implementing risk management and internal control measures in various areas, as well as a means to create a common understanding of risk management and internal controls arising from the organization's operations, enabling the Company to respond effectively to changes in the operating environment.

The Board of Directors of the Group intends for enterprise-wide integrated risk management and internal control to be implemented throughout the organization. The Group recognizes the necessity and importance of risk management and has therefore developed a risk management system for use by employees at all levels across the organization.

The Group has established a Risk Management Department and appointed a Risk Management Committee as well as a Risk Management Working Team to be responsible for the Group's risk management activities. In addition, the Group has established this Risk Management Policy as part of the Group's Risk Management Manual, which has been updated to align with the nature of the Group's business operations.

2. Objective of Risk Management

This Risk Management Policy of the Group has been prepared with reference to the regulations of the Bank of Thailand and best practices in risk management.

2.1 The Group aims to promote risk management in accordance with the enterprise-wide risk management framework by adopting the COSO – ERM framework (The Committee of Sponsoring Organizations of the Treadway Commission, Enterprise Risk Management – Integrated Framework) as a common practice throughout the Group, and to establish risk management as an integral part of decision-making, strategic planning, work planning, and business operations of the Group.

2.2 To establish measures and guidelines for managing residual risks so that they remain within the organization's acceptable risk level, by considering measures to effectively reduce the likelihood and/or impact of potential risks, thereby supporting the achievement of the organization's objectives at both the corporate and departmental levels.

2.3 To enable the identification of unexpected risks or crises and to respond appropriately and promptly in order to minimize losses or damages to the organization.

2.4 To ensure that all departments regularly identify, assess, and manage significant risks, including cases involving significant events, activities, processes, and/or projects that are new or have never been undertaken before, as well as material changes within the organization, taking into account the acceptable level of risk and practical feasibility at a reasonable cost.

2.5 To ensure continuous communication and dissemination of risk management knowledge to executives and employees at all levels, and to develop employees' understanding, awareness of risk ownership, and collaborative risk management within their areas of responsibility.

2.6 The Risk Management Committee has integrated risk management into daily operations and strategic planning, with the objective of balancing risk and return through rigorous risk oversight and fostering a risk management culture that encourages executives and employees at all levels to be mindful of risks, consider the impacts arising from risks, and implement appropriate risk mitigation strategies.

2.7 The Risk Management Committee is responsible for overseeing the Group's risk management to ensure compliance with the policy, as well as providing opinions, recommendations, and follow-up actions to ensure that risk management is efficient and effective.

2.8 The objective of establishing the Group's fundamental risk management policies and control processes is to maintain financial standards, enhance the value of the Group, and ensure that companies within the Group operate under sound standards consistent with the regulatory requirements of the Bank of Thailand.

2.9 Risk management serves as a foundation for good corporate management in driving the organization toward stable growth and business expansion, enabling the Group's business operations to create value and generate appropriate and sustainable returns.

2.10 To ensure that executives and employees at all levels within the organization recognize their responsibilities, which may have an impact on the organization as a whole.

3. Definitions, Meanings, and Terminologies of Risk Management

3.1 “Group of Companies” means Srisawad Corporation Public Company Limited, its subsidiaries, and associated companies in which Srisawad Corporation Public Company Limited directly or indirectly holds shares and exercises control.

3.2 “Supporting Business” means a business having the following characteristics:

3.2.1 Operating activities or functions that directly support or facilitate financial business operations in order to achieve the objectives of financial business operations.

3.2.2 Providing services to other persons, which may include information technology businesses, data research businesses, legal businesses, and asset appraisal businesses. Although such businesses are considered supporting businesses, they may also provide services to the general public; however, the majority of their income must be derived from providing services to the persons specified above when compared to the company’s total revenue.

3.3 “Parent Company” means Srisawad Corporation Public Company Limited.

3.4 “Person with Management Authority” means:

3.4.1 A director, executive of the company, or a person holding an equivalent position under another title, as the case may be.

3.4.2 A person contracted by the company to have authority to manage all or part of the business operations; or

3.4.3 A person who, by circumstances, has the authority to control or dominate the manager, directors, or management of the company to comply with their instructions regarding the company’s policies or operations.

3.5 “Executive Director” means:

3.5.1 A director performing management duties in the position of manager, deputy manager, assistant manager, or any equivalent position under another title.

3.5.2 A director responsible for operations or participating in management in the same manner as an executive, including persons serving on the Executive Committee.

3.5.3 A director authorized to sign binding agreements on behalf of the company, except where such signing relates to transactions already approved by the Board on a case-by-case basis and requires joint signatures with another director.

3.6 “Related Person” means a person having a relationship with another person in any of the following manners:

3.6.1 Being a spouse.

3.6.2 Being a child or adopted child who has not yet reached legal age.

3.6.3 Being a company in which such person or persons under Clauses 3.6.1 or 3.6.2 have management authority.

3.6.4 Being a company in which such person or persons under Clauses 3.6.1 or 3.6.2 control the majority voting rights at shareholders' meetings.

3.6.5 Being a company in which such person or persons under Clauses 3.6.1 or 3.6.2 control the appointment or removal of directors.

3.6.6 Being a subsidiary of a company under Clauses 3.6.3, 3.6.4, or 3.6.5.

3.6.7 Being an associated company of a company under Clauses 3.6.3, 3.6.4, or 3.6.5.

3.6.8 Being a principal, agent, or other person as prescribed by the Bank of Thailand.

Where any person holds shares in any company amounting to 20 percent or more of the total issued shares, whether directly or indirectly, it shall be presumed that such company is a related person of that individual unless proven otherwise.

3.7 "Major Shareholder" means a person who holds shares in excess of 5 percent of the company's total issued shares, including shares held by related persons.

3.8 "Extension of Credit" means lending money or providing personal loan services under supervision.

3.9 "Obligation" means obligations as specified by notifications of the Bank of Thailand.

3.10 "Transactions Similar to Credit Facilities" means hire-purchase transactions and leasing transactions.

3.11 "Intra-group Transactions" means all on-balance sheet and off-balance sheet transactions conducted among companies within the Group.

3.12 "Risk Indicator" means a tool that enables management to determine the level of risk existing at a given time by measuring specified risk factors.

3.13 "Risk Map" means a diagram illustrating the relationships among risk factors within the organization by considering various risk factors and linking the interrelated risks in order to better understand their potential impacts on one another.

3.14 "Risk Management Policy" means this "Policy."

3.15 "Srisawad Group of Companies" means the "Group."

3.16 "Board of Directors" means the "BoD." The Risk Management Committee is appointed by the Board of Directors of the Group.

4. Risk Management Structure of The Group

The Group has established a clearly defined risk management structure, with the Board of Directors responsible for overseeing and ensuring that risk management conducted by management is appropriate and effective throughout the organization. Personnel involved in the Company's risk management consist of officers at all levels, ranging from general employees to the Board of Directors.

The group of companies under Srisawad Corporation Public Company Limited consists of Srisawad Corporation Public Company Limited, 10 directly invested companies, and 10 indirectly invested companies, each of which operates the following businesses:

Name	Business	% Holdings
1. Srisawad Corporation Public Company Limited	▶ Invest in others	-
Directly Invested		
2. Fast Money Co., Ltd.	▶ Secured loans	99.99
3. Srisawad Asset Solutions Co., Ltd.	▶ Holding company	99.99
4. Srisawad Power 2014 Co., Ltd.	▶ Debt collection services, lending services and Insurance brokerage services	99.99
5. Srisawad International Holding Co., Ltd.	▶ Holding company	99.67
6. Srisawad Capital 1969 Plc.	▶ Non-secured loans	72.05
7. P Lending Co., Ltd.	▶ Development of a platform for lending business	75.00
8. Srisawad Digital Co., Ltd.	▶ Digital personal loans	99.99
9. Srisawad Pico Buriram Co., Ltd.	▶ Pico Finance	99.99
10. Srisawad Pico Ubon Ratchathani Co., Ltd.	▶ Pico Finance	99.99
11. Srisawad Pico Nakhon Ratchasima Co., Ltd.	▶ Pico Finance	99.99
Indirectly Invested Through Srisawad International Holding Co., Ltd.		
12. SWP Services Co., Ltd.	▶ Management and advisory services	99.99

Name	Business	% Holdings
13. Srisawad Vietnam LLC	▶ Lending services	70.00
14. Srisawad Leasing Laos Co., Ltd.	▶ Lending services	99.99
Indirectly Invested Through Srisawad Capital 1969 Public Company Limited		
15. S Leasing Co., Ltd.	▶ Hire purchase loans for new motorcycles	90.00
16. Cathay Leasing Co., Ltd.	▶ Hire purchase loans for new motorcycles	99.99
17. Sawad Rung Reung Finance (Cambodia) Plc.	▶ Hire purchase loans for motorcycles in Cambodia	75.00
Indirectly Invested Through Srisawad Power 2014 Co., Ltd.		
18. Srisawad Power 2022 Co., Ltd.	▶ Secured loans	99.99
Indirectly Invested Through Srisawad Asset Solutions Co., Ltd.		
19. SWP Asset Management Co., Ltd.	▶ Asset management	99.99
20. Srisawad Property Solutions Co., Ltd.	▶ Buying and selling and activities related to real estate	99.99
21. Srisawad Property Solutions Casa Co., Ltd.	▶ Buying and selling and activities related to real estate	99.99

5. Roles, Duties, and Responsibilities for Risk Management within the Group

Board of Directors

1. To supervise, acknowledge, consider, and continuously review the Group's risk management to ensure that, overall, the Group has adequate and appropriate risk management practices.
2. To recognize key risks and support management in implementing appropriate risk management throughout the organization in order to assure relevant parties that the Group can effectively manage such risks.
3. To establish a Risk Management Committee for the Group to oversee, monitor, and ensure that subsidiaries within the Group comply with the established risk management policy and with the regulations prescribed by the Bank of Thailand.
4. To prepare and review the Group's risk management policy, which must be approved by the Board of Directors of the parent company and submitted to the Bank of Thailand annually and whenever there are significant changes in the structure or operations of the Group, within 30 days from the date of approval by the parent company's Board of Directors.
5. To establish risk management guidelines for the Group.
6. To ensure that subsidiaries and associated companies within the Group comply with applicable laws, regulations prescribed by regulatory authorities, and policies established by the parent company.
7. To establish an Audit Committee for the Group to supervise and monitor compliance with Group policies and to review the Group's financial reports for accuracy and adequacy.
8. To ensure that the Group has adequate and effective internal control systems and risk monitoring systems.
9. To be responsible for ensuring that there are processes for measuring, managing, monitoring, controlling, reporting, and reviewing risks arising from intra-group transactions at the Group level on a regular basis, at least annually or whenever significant events occur, as well as ensuring adequate disclosure of information relating to intra-group transactions.
10. To disclose policies relating to intra-group transactions and risk management policies associated with such transactions in the annual report.
11. To prepare sufficient information regarding each company within the Group and the overall Group to facilitate inspections and reviews, such as financial statements and significant financial information.

Risk Management Committee

1. To propose the overall risk management policy to the Board of Directors, covering significant risks such as credit risk, market risk, liquidity risk, operational risk, strategic and reputational risk, and other related risks, including:

- Providing recommendations to the Board of Directors regarding Risk Appetite, Risk Tolerance, and Risk Strategy for the Group and business units.
- Providing opinions to the Board regarding the approval of Risk Levels and Risk Concentration within the Board-approved Risk Appetite.

2. To approve significant policies and frameworks for governing risk management, including approving Supplemental Risk Limits and matters relating to Risk Governance as delegated by the Board of Directors.
3. To formulate strategies consistent with the risk management policy, ensuring that the Group's risk levels can be assessed, monitored, and maintained at appropriate levels.
4. To review the adequacy of the Group's risk management policies and systems, including the effectiveness of such policies and systems in terms of risk identification, measurement, aggregation, control, and reporting.
5. To report risk management performance, various risk management activities, and risk mitigation measures to the Board of Directors, as well as report matters requiring corrective actions to ensure effective implementation of the policy.
6. To assess the effectiveness of the Group's risk management and report to the Board of Directors at least once annually, and immediately report any event that may materially affect the stability of the Group.

Audit Committee

1. To supervise and monitor compliance with the Group's policies.
2. To review the Group's financial reports for accuracy and adequacy.

Risk Management Department

1. To prepare and update the risk management policy, framework, and risk management manual as prescribed by the parent company, and submit them to the Risk Management Committee for consideration and approval.
2. To provide information support to the Risk Management Committee in identifying and assessing risks, as well as developing plans and/or additional risk mitigation measures.
3. To collect risk information and risk management approaches from the Risk Management Committee in order to analyze and prepare risk reports, progress reports on plans and risk mitigation measures for submission to the Risk Management Committee, or in cases where significant changes affecting the Group occur, in accordance with the established risk reporting framework.
4. To identify, measure, monitor, and control risks in accordance with the Group's risk management policy, monitor and compare risk management performance against operational plans and established

risk management objectives, including identifying operational issues and obstacles, and report them to the Risk Management Committee.

5. To arrange regular quarterly meetings of the Risk Management Committee and meetings with relevant departments in accordance with the established plans.
6. To support the Risk Management Committee in ensuring that employees throughout the organization understand risks and implement the risk management framework consistently in order to achieve the Group's risk management objectives.
7. To establish clear, efficient, and timely communication channels regarding risk information and the risk management system, including conducting communications, providing guidance, and organizing training on the risk management system for all departments within the Group.
8. To prepare a Risk Map illustrating the interrelationships among risk factors within the organization by considering various risk factors, their interconnections, and underlying causes, in order to provide a clearer understanding of their potential impacts on one another.
9. To conduct the Company's self-risk assessment covering all five risk categories at least once annually at the end of the December accounting period.
10. To prepare and implement a Business Continuity Plan (BCP) to ensure that the Company can continue operating during abnormal events, in accordance with the Company's business continuity management policy and BCP guidelines.
11. To prepare clear operational manuals and procedures for all transactions as operational standards, and to regularly update and review such manuals to ensure they remain current.

6. Risk Management Policy

The Group has established an enterprise-wide risk management system to ensure that the Group can achieve its objectives and enhance operational success in accordance with good governance practices, while effectively responding to the rapidly changing and highly competitive business environment. The Group has established a Risk Management Committee (RMC), comprising directors and senior executives, to formulate management guidelines, develop an effective enterprise risk management system, promote cooperation at all levels within the organization, and oversee overall risk management to ensure that risks remain within the acceptable risk appetite.

The Group's Risk Management Policy covers four key areas as follows:

1. Key Risk Categories Emphasized by the Group

The Group's significant risks consist of five categories: strategic risk, credit and credit concentration risk, market risk, liquidity risk, and operational risk. In addition, companies within the Group are required to prepare a Risk Map to illustrate the relationships among internal risk factors by considering various risk categories, their interconnections, and underlying causes, in order to better understand the potential impacts among such risks, as follows:

1.1 Strategic Risk

Strategic Risk refers to risks arising from inappropriate strategic planning, operational plans, or implementation that are inconsistent with internal factors and external environments, including changes in laws, regulations, and supervisory requirements, the enactment of new laws affecting operational procedures, and the Company's inability to adapt to technological changes. This also includes risks arising from intense competition in the personal loan industry, personal loans secured by vehicle registration, hire-purchase loans, and non-life and life insurance brokerage businesses, which may affect costs, revenues, capital funds, reputation, or the continued existence of the parent company and subsidiaries.

1.2 Credit Risk / Default Risk

Credit Risk refers to the risk of damage arising from counterparties failing to fulfill obligations specified in agreements or contracts, including the risk of counterparties being downgraded, which may affect revenues and operating performance. This includes:

- Lending or transactions similar to lending, such as hire-purchase and leasing transactions.
- Incurring obligations such as guarantees, avals, sureties, and derivative contracts.
- Purchasing or investing in securities issued by companies within the Group.
- Purchasing or selling assets, including repurchase agreements.

Credit risk is considered highly significant because it relates to lending activities, which are the Group's core business transactions. The Group focuses particularly on the following key credit risks:

- **Non-Performing Loan Risk (NPL Risk):** Refers to impaired loans or non-performing loans, including debtors with overdue payments of 90 days or more. This is a major issue affecting

revenues and operating performance. The Group therefore emphasizes prudent lending practices by prioritizing loan quality over loan volume and regularly monitoring loan quality through established policies and procedures.

- **Collateral Recovery Risk:** Certain loan products are secured by automobiles and motorcycles. If the Group is unable to repossess and sell collateral for debt repayment, it may negatively affect the Group's business, financial position, and operating results.

1.3 Market Risk

Market Risk refers to the risk that the Group may suffer losses due to changes in the value of assets, liabilities, and obligations arising from fluctuations in interest rates, exchange rates, equity prices, and commodity prices. The Group's market risk arises from providing financial services to customers, business competition, and service channels.

1.4 Liquidity Risk

Liquidity Risk refers to the risk that the business may be unable to meet debt obligations or contractual commitments when due because it cannot convert assets into cash, cannot obtain sufficient funding, obtains funding at excessively high costs, or relies too heavily on a single funding source. This may affect current and future revenues and operating performance.

The Group manages liquidity risk by assessing cash flows and liquidity positions during periods when funding requirements may differ, in order to support loan maturities, reductions in liabilities, or increases in assets. The Group also maintains contingency plans to address liquidity problems and reviews such plans whenever significant events affecting operations occur.

1.5 Operational Risk

Operational Risk refers to the risk of damage arising from inadequate corporate governance, weak governance structures, or insufficient controls. Such risks may relate to internal processes, personnel, systems, or external events and may affect revenues and capital funds. This includes legal risk but excludes strategic risk and reputational risk.

Key operational risk factors of the Group include:

Internal Factors

- Efficiency of internal processes and internal control systems, including operational procedures supporting business operations and personnel management processes.
- Personnel factors, including adequacy, qualifications, efficiency, and integrity of employees, as well as service quality, customer care, understanding of increasingly complex products and services, and appropriate product sales practices.
- Information systems, including system capability to support business operations, implementation of controls and system audits to limit damages, complexity that may create risks, data security, processing accuracy, and technological changes.

- Loss or damage of contracts or collateral documents due to fire. Contracts and collateral documents are important because they may be used as evidence in legal proceedings; any loss or damage may affect business operations.

External Factors

- External misconduct such as theft, fraud involving assets or information, and money laundering.
- Public disasters, natural disasters, or civil unrest that may damage Group assets and affect customers' ability to repay debts.
- Amendments to regulations or the issuance of new domestic and international regulatory requirements that are becoming increasingly stringent worldwide.
- Cyber Risk or information technology threats, which are rapidly increasing in complexity and diversity amid the transition toward the digital era.
- Risks arising from epidemics or pandemics, which directly affect the lives and health of customers and employees and impact both asset quality and operational efficiency.

1.6 Risk from Major Shareholder Concentration

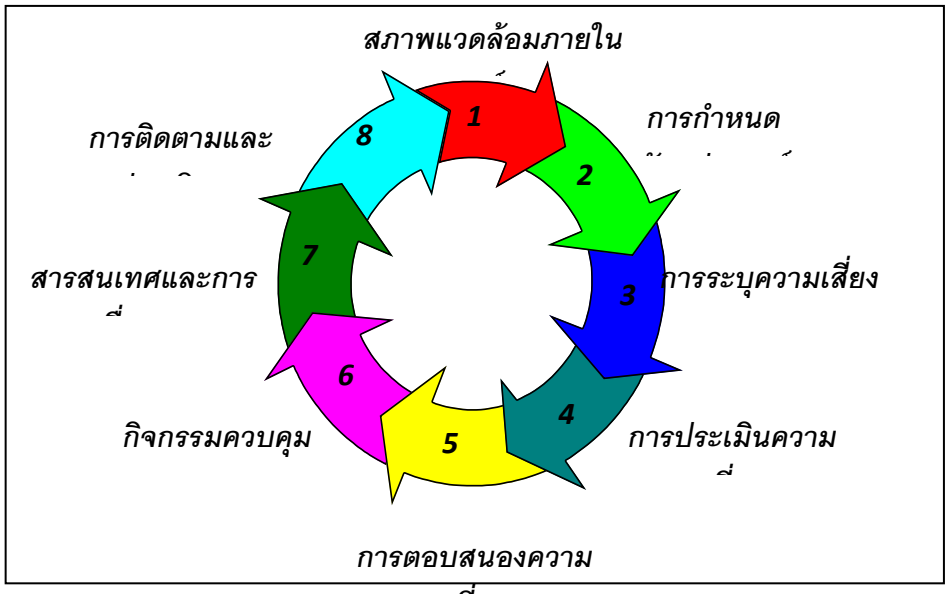
This refers to the risk arising from a major shareholder holding a significantly larger shareholding than other shareholders, enabling such shareholder to control voting at shareholders' meetings and potentially obstruct checks and balances on agenda items proposed by shareholders.

2. Risk Management Framework and Process of the Group

The Company's risk management framework and process are based on internationally recognized risk management standards, namely COSO ERM (The Committee of Sponsoring Organizations of the Treadway Commission, Enterprise Risk Management – Integrated Framework 2017) and ISO 31000: Risk Management, to serve as common guidelines for executives and employees across the organization.

The Company's risk management process consists of eight key steps as follows:

Risk Management Framework in Accordance with the COSO Framework



1) **Internal Environment**

The internal environment is a fundamental component of the risk management framework, influencing the organization's strategy setting, objective setting, activity design, as well as risk identification, assessment, and management. The internal environment refers to various factors such as ethics, management and employee working approaches, management style, and the delegation of authority and responsibilities. Management must jointly establish these together with employees throughout the organization in order to create awareness, recognition, and understanding of risks and controls among all employees.

2) **Objective Setting**

The Company establishes clear business objectives to ensure that such objectives are aligned with strategic goals and the level of risk acceptable to the organization, by managing operations within the framework of Risk Appetite and Risk Tolerance.

3) **Event Identification**

In the event identification process, all risk factors that may arise should be considered, such as strategic, financial, personnel, operational, legal, tax, system, and environmental risks, including relationships among potential events and sources of risk from both internal and external environments.

- External Environment

The external environment consists of factors outside the organization that influence the organization's objectives/goals, such as:

- Culture, politics, laws, regulations, finance, technology, the economy, and competitive environments both domestically and internationally
- Key drivers and trends affecting organizational objectives
- Acceptance and values of external stakeholders

- Internal Environment

The internal environment consists of factors within the organization that influence organizational goals, such as:

- Organizational capabilities in terms of resources and knowledge, including capital, time, personnel, processes, systems, and technology
- Information systems, information flow, and formal and informal decision-making processes
- Internal stakeholders
- Organizational policies, objectives, and strategies
- Organizational perceptions, values, and culture
- Standards and models developed by the organization
- Organizational structure, including management systems, roles, duties, and responsibilities

4) **Risk Assessment**

Risk assessment is a process that follows risk identification and consists of the following key processes:

1. Risk Analysis

This involves considering the causes and sources of risk, both positive and negative consequences, as well as the likelihood of such consequences occurring. Factors affecting both impact and likelihood must be identified. One event or circumstance may create multiple consequences affecting several objectives/goals. The analysis should also consider existing risk management measures and their effectiveness.

2. Risk Evaluation

Risk evaluation compares the level of risk derived from the risk analysis against the acceptable risk level (Risk Appetite). If the risk level exceeds the acceptable threshold, such risk must be managed immediately.

3. Risk Criteria Determination

The criteria used for risk assessment should reflect the organization's values, objectives, and resources. Certain criteria may be developed based on legal requirements or regulatory standards imposed by supervisory authorities or membership organizations. The criteria established must align with the organization's risk policy and be reviewed continuously.

Factors considered in establishing risk criteria include:

- Nature and type of potential impacts and methods for assessing impacts
- Methods for determining likelihood
- Timeframes of likelihood and impacts
- Methods for determining risk levels
- Acceptable risk levels
- Risk levels requiring management action

Likelihood

The likelihood of risk events and the level of damage are categorized into five levels, with specific definitions assigned to each level.

Level	Description
5	Almost certain
4	Likely
3	Possible
2	Unlikely
1	Rare

Impact

The impact of risk events is categorized into five areas:

1. Financial impact
2. Reputational and corporate image impact
3. Regulatory and compliance impact
4. Personnel impact
5. Impact from delays in critical projects

Each category is divided into five levels, with definitions specified for each level.

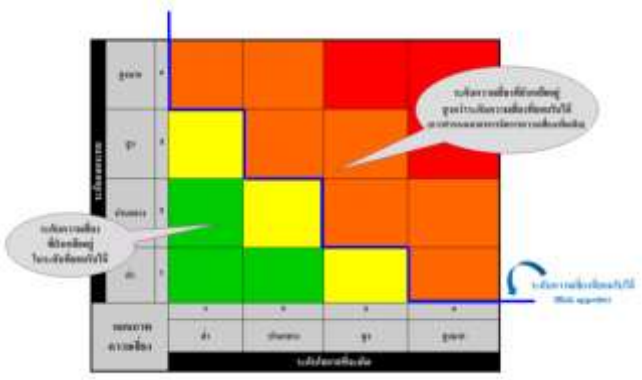
Level	Description
5	Critical
4	Significant
3	Moderate
2	Minor
1	Insignificant

Risk Map

A Risk Map is a tool used to report assessed risk levels by illustrating the relationship between the likelihood of risk occurrence and the impact of the risk. It consists of two axes:

- Risk Impact Axis
- Risk Likelihood Axis

This is used to prioritize risks into categories of high risk (red), relatively high risk (orange), moderate risk (yellow), or low risk (green).



After the assessment results are obtained, the Risk Management Department shall:

- Analyze and summarize the assessment results using the Risk Map and prioritize risk issues
- Present the assessment results to the Risk Management Committee for selecting key risk issues requiring management attention and assigning responsible management units to establish additional risk management measures beyond existing controls
- Present risk issues and additional required management measures to the Risk Management Committee, Audit Committee, and Executive Committee for acknowledgement

5) **Risk Response**

After the Company identifies organizational risks and assesses their significance, appropriate responses must be implemented to reduce losses or the likelihood of impacts to levels acceptable to the organization.

6) **Control Activities**

Control activities are policies and operational procedures established to ensure that risks are managed within acceptable levels and to prevent impacts on organizational objectives. Control activities vary and may be categorized into four types:

1. **Preventive Controls** – controls designed to prevent risks and errors from occurring at the outset
2. **Detective Controls** – controls designed to detect errors that have already occurred
3. **Directive Controls** – controls designed to encourage or promote achievement of desired objectives
4. **Corrective Controls** – controls designed to correct errors that have occurred and prevent recurrence in the future

Control activities should also consider cost-effectiveness by balancing costs against expected benefits.

7) **Information and Communication**

Effective information and communication systems are essential for organizations to identify, assess, and manage risks. Relevant information from both internal and external sources should be properly recorded and communicated to personnel in an appropriate format and timeframe to enable them to perform their duties and responsibilities effectively. This also supports risk management reporting so that everyone within the organization is aware of existing risks and the results of risk management efforts.

Effective communication includes top-down, bottom-up, and cross-functional communication. Risk management should utilize both historical and current information. Historical information indicates trends and helps forecast future performance, while current information assists management in assessing risks arising within processes, business lines, or departments, enabling the organization to adjust control activities as necessary to maintain risks within acceptable levels.

8) **Monitoring**

The internal risk management process must include communication regarding risk assessments, controls, progress in risk management, monitoring of key risk trends, and abnormal incidents on an ongoing basis to ensure that:

- Risk Owners regularly and appropriately monitor, assess, analyze, and manage risks under their responsibility

● Risks significantly affecting the achievement of organizational objectives are reported, including risk management progress and risk trends, to responsible management and the Risk Management Committee

● Established internal control systems are adequate, appropriate, effective, and actually implemented to prevent or mitigate risks, with continual improvements made to align with changing circumstances or risks

The Risk Management Department shall report risk status and risk management processes to the Risk Management Committee for acknowledgement and consideration.

● Risk Assessment Process for Companies within the Group. Each company within the Group should conduct a self-assessment covering at least five risk categories: strategic risk, credit risk, market risk, liquidity risk, and operational risk, at least once annually at the end of the December accounting period. The self-assessment must be approved by the company's Board of Directors or Executive Committee and submitted to the parent company so that the Group Risk Management Committee can evaluate the Group's overall risk management performance and report to the parent company's Board of Directors at least once annually.

● Process for Establishing the Group's Risk Management Policy. The establishment and review of the Group's risk management policy must be approved by the parent company's Board of Directors and reviewed at least once annually and whenever significant changes occur. The policy must also be reported annually to the Bank of Thailand within 30 days from the date of approval by the parent company's Board of Directors.

● Compliance with the Group's Risk Management Policy

1. Companies within the Group and all departments related to risk management must strictly comply with the Group's risk management policy.
2. Any operations not in compliance with the Group's risk management policy must obtain approval from the parent company's Board of Directors, committees or units delegated by the Board, or relevant regulatory authorities, as applicable.

3. Risk Control and Management of the Group

After risk assessment, appropriate risk control methods or measures must be established. A good control system should be easy to implement, cost-effective, and should not negatively affect work processes or quality. The control system must also clearly reduce risks.

Risk management methods should be practical and consider the cost-benefit relationship, while also taking into account acceptable risk levels.

Risk management methods may include one or a combination of the following approaches:

1) Risk Acceptance (Take/Accept)

Accepting the risk without taking additional action to reduce likelihood or impact because the residual risk level is low, acceptable, or the cost of management exceeds the expected benefits.

2) Risk Treatment/Reduction (Treat/Reduce)

Reducing the likelihood and/or impact of risks by adjusting operations or preparing supporting plans, such as modifying work processes, implementing monitoring measures, restructuring, or employee training.

3) Risk Transfer/Sharing (Transfer/Share)

Reducing the likelihood and/or impact of risks by transferring or sharing responsibility with others, such as through insurance, transferring responsibility to contractors, outsourcing, or concession arrangements.

4) Risk Avoidance (Terminate/Avoid)

Eliminating or avoiding risks due to their high likelihood and severe impact, such as changing objectives, canceling projects or plans, or changing project execution methods.

The selection of risk management strategies must consider the underlying risk factors as well as the costs or resources required compared to expected benefits to determine whether the strategy is worthwhile. Once an appropriate strategy is selected, the responsible department must prepare a risk management plan to facilitate monitoring and evaluation of risk management results.

The parent company also has a policy of appointing executives as directors of each company within the Group for governance purposes and requires each Group company to prepare business plans to ensure operational policies align with Group policies.

4. Business Continuity Management (BCM) and Business Continuity Plan (BCP)

Business Continuity Management Policy (BCM/BCP)

In the current environment, all companies continue to face risks beyond the five categories outlined in this policy. These risks arise from unexpected external factors beyond control, such as natural disasters, fires, terrorism, and pandemics. Therefore, the Group requires measures to mitigate the severity of such events through Business Continuity Management (BCM) and Business Continuity Plans (BCP) to minimize impacts on Group companies and restore operations to normal within an appropriate timeframe.

Objectives of Business Continuity Management

(1) To ensure that Group companies are prepared to respond to unforeseen damaging events.

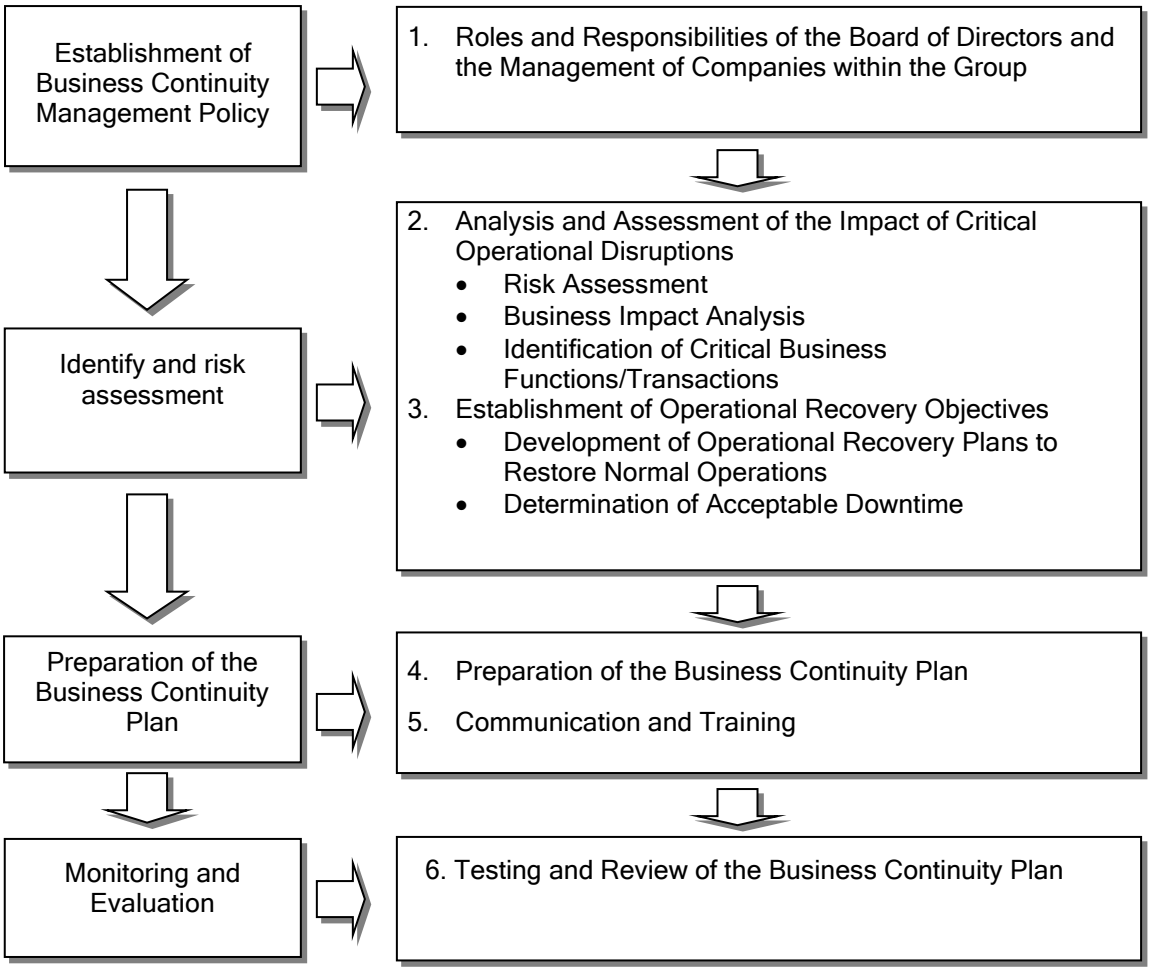
(2) To provide operational guidelines during damaging events in order to control and mitigate damages and minimize impacts on Group companies, including financial, legal, reputational, and market share impacts.

(3) To ensure that, in the event of severe incidents or crises, critical products/services and operations of Group companies can continue operating or, if interrupted, can resume within an appropriate period.

(4) To ensure that shareholders, customers, employees, and stakeholders have confidence in the stability of the Group in the event of a crisis.

Components of Business Continuity Management (BCM)

Companies within the Group shall establish components of Business Continuity Management in accordance with the framework and details set out below:



1. The management of each company within the Group shall be responsible for establishing business continuity management strategies and policies, and for allocating sufficient resources to support implementation. Management shall also consider business continuity risks and ensure compliance with the Business Continuity Plan (BCP). Senior management shall clearly define the chain of command and the responsibilities of all relevant parties. Companies with complex business operations may establish a dedicated unit to oversee business continuity management. In this regard, the business continuity management policy shall be reviewed at least annually or whenever there are significant changes in relevant factors, and the parent company must be informed of every review or amendment.

2. The Group shall conduct risk assessments, including analysis and assessment of the impacts of disruptions to critical products/business functions, in order to prioritize operations and allocate resources effectively for operational recovery. This process shall cover the following matters:

a) Risk Assessment

Companies within the Group shall assess risks that may cause disruptions to critical products/business functions at least once a year or whenever there are significant internal or external changes that may affect the Group. In addition, existing risk control processes shall be analyzed, and processes and necessary resources shall be improved and prepared to manage risks that could result in operational disruptions.

b) Business Impact Analysis (BIA)

Companies within the Group shall analyze the business impacts arising from incidents that may disrupt critical products/business functions in order to understand the interdependencies of such functions and the impacts of disruptions. The analysis shall be used to prioritize operations and allocate recovery resources. Consideration shall include both quantitative and qualitative impacts on stakeholders, such as potential revenue losses, additional expenses, reputational damage, and loss of credibility.

c) Identifying Critical Products/Business Functions

After conducting the Business Impact Analysis, companies within the Group shall use the results to identify critical products/business functions that, if disrupted, could significantly affect operations, reputation, and business performance.

3. Recovery Objectives shall include establishing a Recovery Strategy to restore operations to normal conditions. The strategy shall be based on the results of the Business Impact Analysis, and adequate budgets and resources shall be allocated to support implementation. Insurance coverage may also be considered as a means to mitigate losses. However, insurance alone shall not be deemed a substitute for business continuity management, since the primary objective of insurance is not to restore business operations to normal conditions.

In addition, Recovery Time Objectives (RTO) shall be established. Companies within the Group shall determine acceptable downtime for each critical product/business function, prioritize such functions, and specify the required recovery timeframes. The determination of acceptable downtime must be approved by the Board of Directors and senior management.

Business Continuity Plan (BCP)

Companies within the Group shall prepare a written Business Continuity Plan (BCP) specifying procedures for responding to or recovering from disruptions in order to restore operations to normal conditions and ensure continuous business operations. The plan shall include at least the following:

1. Detailed operational procedures in the event of disruptions to critical products/business functions so that operations can resume within the specified timeframe.
2. Resources required for operations, such as personnel, computer equipment, communication devices, contractual documents, and insurance policies.
3. Communication plans for internal and external stakeholders.
4. Plans for establishing alternate operating sites where necessary. Such sites should be sufficiently distant from the primary operating site to avoid being affected by the same incident, should not rely on

the same utility infrastructure, and should be readily available for use at all times. However, companies within the Group with relatively limited transaction volumes may use other offices/branches as substitute operating locations instead of establishing dedicated alternate sites, provided that appropriate contingency procedures are in place.

5. If companies within the Group rely on key service providers, they must ensure that the service providers' Business Continuity Plans are aligned with the Group's Business Continuity Plans.

Communication, Training, and Testing

The Group shall establish communication plans specifying procedures and methods for communication, while considering the impacts on both internal and external stakeholders in the event of operational disruptions. This is to ensure timely notification and prevent panic.

Regular training and communication regarding the Business Continuity Plan shall also be conducted to ensure that employees and relevant parties understand their respective roles and responsibilities, and to reinforce confidence that companies within the Group can continue providing services without interruption.

BCP Testing and Reviewing

The Group shall conduct regular testing and reviews of the Business Continuity Plan (BCP Testing and Reviewing) at least once a year, or whenever there are significant changes in factors affecting operational disruption risks. This is to ensure that the plan remains effective and practical. Relevant personnel at all levels shall participate in such testing, and the results shall be reviewed and used to improve the effectiveness of the plan. The testing results shall also be reported to senior management and the relevant committees.