Risk Management Manual

Organizational risk management policy framework

To ensure that the operations of Muangthai Capital Public Company Limited are in accordance with the principles of good corporate governance build stability for sustainable business the performance was in accordance with the goals set. All executives and employees are involved in awareness, awareness, and understanding of various risks including the risk of corruption that may occur, and can find ways to manage risks to prevent or reduce the risk to an acceptable level.

Muangthai Capital Public Company Limited would like to announce the risk management policy for general acknowledgment as follows.

1. All executives and employees are responsible for risk management throughout the organization with systematic and continuous management have the same standards.
2. All executives and employees must implement risk management as part of their normal operations both in the strategic planning process, decision making, and day-to-day tasks by applying information technology for maximum benefit.
3. All executives and employees must report the assessed and prioritized risks as well as specifying risk management methods and responsible person (Risk owners) by this report must be presented to the supervisor in a hierarchical order.
4. Identification and management of risks affecting the achievement of the company's objectives must be managed in a systematic way to keep the risks at an acceptable level and prevent unforeseen losses to the business as well as take advantage of the opportunities that exist this is to create a balance of business growth, risks, and rewards of the company.

5. Assessment of risk management by reviewing and continually participating in the improvement and development of the risk management system to be efficient and effective.
6. Risk owners must report risks to the board and the executive committee in accordance with the periodic risk level through the channels specified in the risk management manual.

The risk management policy may be revised and changed to ensure that this policy is still appropriate and can be implemented effectively in the future.

The relationship between growth risk and reward

Risk management does not imply risk tolerance. Therefore, a company takes a certain degree of risk in formulating strategies to create and maintain its value by considering the financial returns that are appropriate for that level of risk as well.

The company's risk management framework this enables the company to systematically identify and assess risks and determine the acceptable risk level consistent with the growth and return objectives risk management is a part of creating sustainable value for the company linking effective risk management to achieving objectives this allows the company to reduce business uncertainty which ultimately affects the improvement of the company's performance.

The company's objectives and business environment are constantly evolving. This results in a change in the company's risks as well. A good company's risk management system relies on the careful and consistent assessment of the company's risk characteristics and extent if there is good risk management, it will create added value for the company is to manage and control risks to an acceptable level it's not about eliminating all risks.

Risk Management Structure

Company's risk management structure there are new job duties that were not in the normal structure, namely.

- The risk management committee is the person who sets the risk management policy follows up on the implementation of the management plan risk to practice assesses the adequacy of risk management plans and reports critical risks to the board of directors.
- Risk management working group is a supporter of each party in order to be able to implement the policy by providing knowledge give advice on how to proceed to collect and analyze risk information as a whole of the company and collect reports to send to the risk management coordinator to report directly to the risk management committee for presentation to the board of directors.
- Risk management coordinator is the secretary of the risk management committee risk acting as coordinator in departments closely in order to be able to implement the risk management policy in the department and report take the risk to the superiors in the hierarchy including reporting to the risk management committee.

This established risk management structure is a combination of risk management activities with the normal management of the company.

- **The person who is directly responsible for risk management** is the person who performs the normal work in every unit, comprising the Board of Directors, Board of Directors Managing, Director Deputy Managing, Director Assistant Managing, Director Department Manager, Branch Managers, Department Heads, and all employees will be the one who performs the specified assess and define measures to manage risks.
- **The person responsible for technical support and advice on risk management** is the one who presents the framework risk management as a guideline for internal company practice collect, monitor and review the suitability in risk management including providing support in

various fields to create awareness and understanding of the importance of risk management consists of the risk management committee the risk management working group and the risk coordinator.

- **The person responsible for reviewing the risk management process** is the person who reviews the efficiency and effectiveness of the risk management committee risk management process the risk management process is a business process and must be reviewed just like any other task consisting of the audit committee and internal audit unit.

Roles and responsibilities of personnel involved in risk management

Risk management is an ongoing task and is part of the daily work roles and responsibilities of management and employees at each level the details are as follows.

Board of Directors and/or Executive Committee

- Approve risk management policy and anti-corruption policy and the level of risk acceptable to the company.
- Oversee the risk management to ensure that the risk management policy is effectively and continually implemented.
- Monitor the company's major risks to ensure that the risks are managed to an acceptable level.
- Consider the overall risks of the company and compare them with the acceptable risk levels.
- Receive a report from the board of directors managing risks related to the implementation of risk management policies.

Risk Management Committee

- Present to the board of directors to formulate risk management policies and acceptable risk level.
- Assess the risks of corruption, which the company attaches importance to operations and to be clear in the implementation, to set effective measures to prevent and reduce risks, including monitoring, evaluating and reporting results.
- Review the risk management report and take steps to ensure that the risk management is adequate and appropriate able to manage risks to an acceptable level and risk management has been implemented continuously.
- Coordinate with the audit committee regularly by exchanging knowledge and information about risks and internal control that has an impact or may have an impact on the company.
- Any other actions related to risk management as assigned by the board of directors.
- Meeting of the risk management committee at least twice a year, depending on the company's major changes such as market expansion to neighboring countries, the establishment of additional subsidiaries, etc.

Risk Management Working Group

- Presenting strategies and business plans to the managing director as well as identifying important risks that may affect the strategy and business plans, including the risks of corruption.
- Implement risk management policies and frameworks that have been approved by the board of directors to develop operations in the line of command for which they are responsible.
- Support the executive committee in carrying out the assigned duties and responsibilities.

- Reviewing the risks and managing risks under the chain of command for which they are responsible.
- Promoting the establishment of a risk management culture and appropriate internal control within the chain of command for which they are responsible.
- Coordinate with Executive Directors or other departments to exchange risk information and find a way to manage risks that maximize benefits to the company.
- Advise the team in the responsible department on key issues that arise in the Risk Management process.
- Coordinate risk management to ensure consistent practices across the company.
- Support the development of a risk management framework including the implementation and continuous monitoring.
- Coordinate with the preparation and update the company's risks.
- Coordinate training on risk management.
- Ensure continuous effective risk communication.

Managing Director

- Presenting strategies and business plans to the company's directors as well as identifying key risks that may affect the strategy and business plans, including risks arising from corruption.
- Implement risk management policies and frameworks that have been approved by the board of directors to develop company-wide.
- Take action to ensure that the business strategy is attainable under the risk policy approved by the board of directors.
- Operates to ensure that risk management is continually implemented throughout the company.
- Supports an appropriate culture of risk management and internal control.

Risk Coordinator

- Coordinates the identification and management of common risks and the risks arising from corruption appropriately within responsible agencies.
- Provide advice to various departments on risk management techniques.
- May act as a risk coordinator (Facilitator) in the risk management workshop in case of request.
- Collect and analyze the risks of the responsible department and departments in the risk management working group presented to the managing director and the risk management committee.
- Coordinating with the risk management working group and taking steps to ensure that risks related to other departments are appropriately managed.
- Follow up on the progress of the risk management action plan in the responsible departments and the departments in the working group manage risks by regularly reporting to the managing director and risk management committee.

Executives and all employees

- Identify and manage risks as part of daily operations and continuity in accordance with the framework manage company risks.
- Regularly monitor the management of risks associated with their job responsibilities.
- Report critical risks and problems arising in risk management to supervisors in a timely manner accordingly.

Audit Committee

- Operates to ensure that there is an appropriate internal control system to deal with general risks and risks arising from the company's corruption.
- Conduct independent reviews to ensure that general risk management and the risks arising from corruption are effectively treated with appropriate improvements.

- Coordinate with the risk management committee for information about general risks and risks arising from corruption and internal controls that have an impact or may have an impact on the company and assigned to an inspection agency internally, plan and monitor such risks.
- Clarify the effectiveness of internal control and key risk management to the board of directors for consideration.

Internal Audit Unit

- Supporting the board of directors audit committee and senior management in the performance of the review general risk management process and risks arising from corruption and internal control, and give recommendations to improve the risk management process to be sufficient and effective.
- Conduct reviews to ensure that internal controls are properly implemented to manage the company's risks.
- Take general risk information and risks arising from corruption from the overall Risk Management process both identifying issues that the board and senior executives focus on planning risk.
- Based audit work may have impact on the company.

Definition of Risk Management

1. Risk

Means an uncertain event this has the potential to happen in the future and has both positive and negative impacts. If it is negative, it will lead to mistakes, damages, leaks, waste or undesirable events causing the company's operations to fail to achieve the stated objectives. Therefore, it is necessary to consider the likelihood of the event and the impact it will receive.

2. Risk Factors

Means the cause or cause of the risk which will not achieve the objectives according to the main operating procedures set forth. The company aims to operate the business to add value to the shareholders arising from external and internal factors is a risk factor which should identify the root cause in order to properly analyze and formulate strategies/measures/guidelines to reduce risks appropriate to the situation and culture of the organization.

Internal factors such as

- Technological risk factors such as inappropriate use of technology technological lagging due to technology newborn fast failure of technology that is too new, etc.
- Operational risk factors such as shortage of personnel changes in operating personnel, shortages of resources, uncertainty in demand (demand), uncertainty in not receiving the requested budget operation process are not suitable, etc.
- Organizational culture factor.
- Personnel ethical facto.
- Working environment factor.

External factors such as

- Political and social risk factors such as continuity in government policy.
- Financial and economic risk factors such as economic volatility, oil prices, interest rate fluctuations inflation volatility exchange rate fluctuations, etc.
- Legal risk factors such as the ambiguity of the relevant laws changes in rules and regulations that are lagging behind changes in related resolutions, etc.
- Environmental risk factors and natural disasters such as insurgency, war, floods, typhoons, mudslides, earthquakes, droughts, epidemics, etc.
- Risk factors for trading partners or co-investors.
- Risk factors from corruption from any action whether it is bringing the part of making

promises, requests, and claims giving or receiving cash or items instead of cash or property or any other benefits including all forms of bribery with government officials or any other person either in government or documents whether directly or indirectly for such persons to perform or except for duty to obtain or maintain any other unfair business interests.

These risk factors led the management to consider how much uncertainty the company would accept so that the company can maintain or increase the value of the shareholder management should understand the impact of events, both positive and negative, and manage them to add value damage reduction and reduce the uncertainty of the overall performance effective risk management can help identify and assess risks at all levels of a company and can help assess the likelihood and impact of risks on the company's value more reliable.

Uncertainty can affect a company both negatively and positively. This means risk or opportunity that could destroy or add value to the company. Risk management should initiate a consistent understanding of the definition of risk so that everyone can see risks and opportunities in the same direction.

For the occasional event, it supports or increases the company's value. Management should take steps to ensure that opportunity events can be identified and be taken into account in conjunction with the company's strategic planning or to be attributed to the determination of the company's objectives so that the company can take advantage of those opportunities to create added value for the company.

Therefore, the company should take steps to avoid or minimize any incidents that may cause damage and try to identify events that are opportunities to add value to the company.

3. The nature of the risk

Risks can be classified into 4 types as follows.

3.1 Strategic Risk means risk arising from policy-making and strategic planning including improper implementation or inconsistency with various factors both internal and external factors this may affect the direction of development and the achievement of goals and/or goals of the company.

3.2 Operational Risk means the risk that occurs in every normal working process it covers the factors involved in the process information technology material/equipment working personnel that there is a control system check how good it is, which if not good enough. The company has to find a way to prevent that risk from occurring. Otherwise, it may affect the success of the implementation of the company's action plan or strategic plan. including corruption resulting from the practice or neglect of duty or abuse of power in office in any form, fraud, concealment, concealment of evidence in order to obtain unworthy benefits or embezzlement which affects the efficiency of the work process.

3.3 Financial Risk means the risk arising from unpreparedness in financial matters budget and various expenditure control excessive or ineffective including account decoration by refraining from providing information or intentionally giving false information in the company's financial status report.

3.4 Compliance Risk means the risk arising from failure to comply with the regulations or relevant regulations or existing rules that are inappropriate or impede the performance or unable to comply with the specified time and may affect penalties in accordance with applicable laws as well as tracking compliance results with relevant rules or regulations.

4. **Risk Assessment** means the process of identifying risks and analyzing to prioritize the risks that will affect the achievement of the organization's goals by evaluating likelihood and impact.

- Likelihood refers to the frequency or likelihood of an event, risk
- Impact refers to the magnitude of the damage that will happen if risk event.
- Degree of Risk means the state of the risk assessed opportunity and impact of each risk factor are divided into 5 levels: very high risk, high risk, medium risk little risk and very little risk.

Opportunity		Effect			
		Operate	Damage assessment	Image	IT
5	•every week •more than 100 per month	An interruption of operations or continued use of the services for an extended period exceeding the SLA or Beneficiary Engagement or much longer than the marker average or cause serious damage to stakeholders or beneficiaries.	More than 10 million baht	There was negative news in the media for more than 5 consecutive days	There was a major problem and a lot of damage causing the system to stall for more than 1 day
4	•every 2 weeks •76-100 times per month	There has been a disruption of operations beyond the SLA, but the stakeholders are still accrptable and there is no catastrophic damage to the stakeholders and the risks can be managed to minimize the next time.	More than 500,000 baht but not more than 10 million baht	There was negative news in the media for more than 4-5 consecutive days	There was a major crash and some damage causing the system to stall for more than 1 day
3	•every 1-3 months •51-75 per month	The interruption of operations doed not exceed the SLA, is in anobligation with a stakeholder, or is close to the acceptable average of the system or stakeholder.	More than 200,000 baht but not more than 500,000 baht	There was negative news in the media for more than 3 consecutive days	There is a problem that affects the work process but can be fixed within days
2	•every 1-6 months •26-50 times a month	The interruption of operations does not exceed the SLA, or is in an obligation with a stakeholder, or is close to the acceptable average of the system or stakeholder.	Morn than 50,000 baht but not more 200,000 baht	There was negative news in the media for more than 2 consecutive days	There is a problem that affects the work process but can be fixed within 1 hour
1	•every 6-12 months •1-25 times per month	No interruption of operations or use of the services of the stakeholders.	less than or equal to 50,000 baht	There was negative news in the media for more than 1 consecutive days	a little problem but does not affect the work process

5. **Risk Response** means a method to reduce the likelihood of an incident or risk or reduce the impact of damage from a risk event to an acceptable level (Risk Tolerance) by choosing an approach at will deal with that risk Management must consider the cost or cost of managing that risk compare with the benefits that will be obtained are appropriate and worth it or not risk management In the event that it is a risk caused by external factors which are not under

the control of the management Preventing or reducing risks can be done as follows.

5.1 Risk reduction or reduction in the likelihood of risk is an attempt to reduce the risk by adding or altering certain phases of an activity or project that would lead to a risky event or reduce the likelihood that a risky event will occur, for example, training personnel to have sufficient knowledge, assigning contractors and contractors to separate or reduce the severity of the impact when a risky event occurs, such as installing a fire extinguisher backing up and saving periodic backups.

5.2 Risk-sharing or transfer of risks is the transfer of some risks to others/other departments to be jointly responsible. When a risk event occurs, the effects must be shared the risk-sharing does not reduce the risk that will occur but it is a guarantee that when the damage is done, the organization will be compensated by others, such as insurance (Insurance), contracts (Contracts), warranties (Warranties), outsourcing.

5.3 Risk Accept means taking risks to manage by yourself within the agency if the analysis shows that there is no proper risk management method. This is because risk management costs are higher than benefits. However, measures should be closely monitored to mitigate the consequences.

5.4 Risk Avoidance is the negation and avoidance of potential risks by halting, canceling, or altering the activities or projects that lead to it a risky event, but there is a disadvantage, namely, that it may affect the change in the organization's plans too much and unable to achieve the goals set if it is a risk related to internal control caused by internal factors which are under the control of the management Prevention or reduction of risks can be done by providing adequate and appropriate control activities.

6. **Enterprise Risk Management** means managing factors and controlling activities including various operational processes to reduce the cause of each chance that the company will cause damage the level of risks and impacts that will occur in the future are at the level acceptable to the company, assessable, controllable, and systematically audited by taking into account the achievement of goals, strategies and reputation of the organization as important supported by and participation in risk management from departments at all levels throughout the company.

7. **Internal Control** is a policy and practice that will help ensure that the risk response guidelines have been implemented control activities occur at all levels all functions and throughout the company control the operation of the unit to be effective and effectiveness.

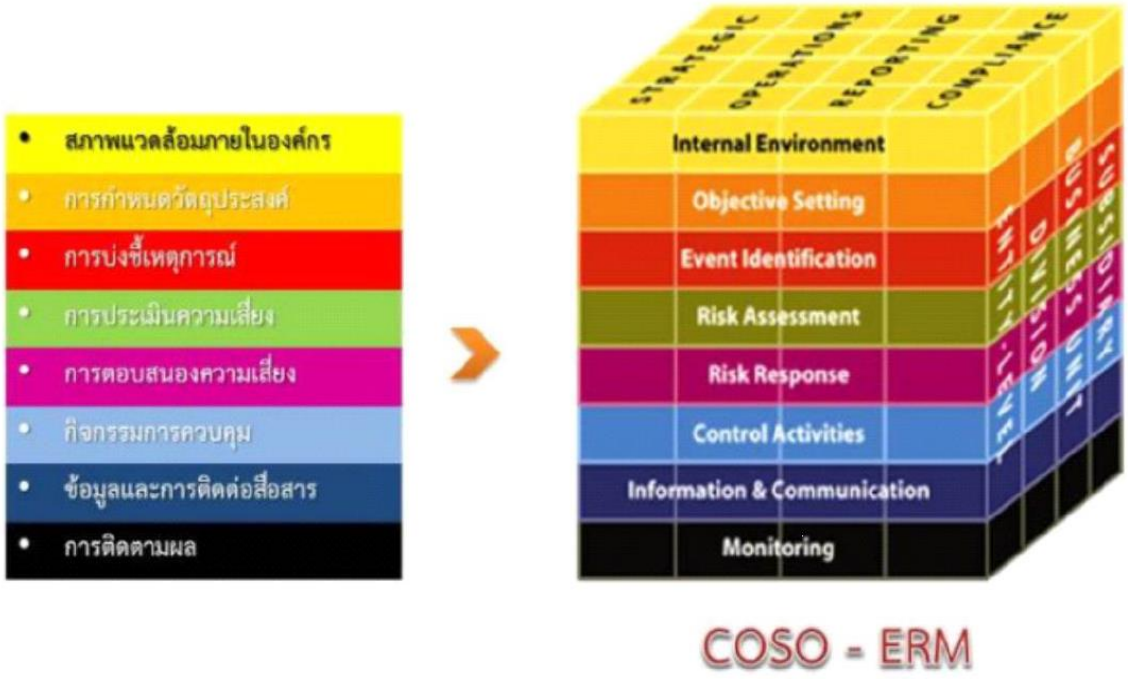
8. **Monitoring and evaluation** mean the process of evaluating the quality of performance and continuously and regularly assess the effectiveness of the established internal controls to ensure that the established internal control and risk management systems are adequate and appropriate there are real practice defects found to be corrected appropriately and in a timely manner.

9. **Goals of the organization (Goal)** refer to the needs of the strategic planner or management wants it to happen as expected both problem-solving (Problematic Goal) and development (Development Goal).

Risk management process

Enterprise-wide Risk Management ERM (Enterprise Risk Management) is the process of identifying and analyzing. Risk in the perspective of a holistic, integrated and company-wide image it covers all activities leading to the achievement of goals such as Strategic Goals, Operations Efficiency and Effectiveness, reporting and compliance.

Risk Management by adhering to risk management principles in accordance with the guidelines of The Committee of Sponsoring Organizations of the Treadway Commission - Enterprise risk management (COSO-ERM). Risk management according to this guideline consists of 8 elements related to business operations and management processes as follows:



From the dice picture above each topic can be described as follows:

1. **<u>Internal environment (Internal Environment)</u>**

Is an important basis for the framework of risk management this environment influences the formulation of organizational strategies and goals scheduling activities assessment indication and risk management the internal environment of an organization consists of many factors such as ethics, the way management and personnel work including the philosophy and culture of acceptable risk management (Risk Appetite) is an important part of the internal environment of the organization and affects the determination strategies to implement the organization to achieve both return and growth goals each strategy has its own risks related differently.

Therefore, risk management thus helping executives to formulate strategies with acceptable risks for the organization.

2. Objective Setting

Clear objectives are the first step in the risk management process. The organization should ensure that the objectives established are consistent with its strategic goals and acceptable risks. In general, objectives and strategies it should be recorded in writing and can be considered in the following areas:

2.1 Strategy, related to the overall goals and mission of the organization.

2.2 Operational aspect related to efficiency, performance and profitability.

2.3 Reporting Involves both internal and external reporting.

2.4 Compliance relating to compliance with laws and regulations.

Objectives are defined on two levels.

- Organizational objectives it is the objectives or operational goals of the organization as well as affecting operational goals.
- Departmental objectives and main process It is the objective of each of the main operational steps to meet to achieve the success of the organization's objectives.

The objectives must be consistent across the company to ensure that departments, executives and employees are working to achieve company objectives by reducing activities, processes and departments unnecessary objectives must be clear and feasible based on a principle known as SMART, which states that a good objective must have the following characteristics.

1) Clear (Specific) Objectives should clearly state the desired rewards or results so that everyone can understand.

2) Measurable Objectives must be measurable and specify the criteria for measuring the results if the objectives are not measurable the company should consider activities related to the objectives and the size of the investment in that activity instead.

3) Achievable objectives or expectations must be feasible based on current events, timing, and resources allocated.

4) Relevant the objective returns or outcomes must be consistent with the objectives of other parts of the company.

5) The time-bound must be clearly stated when the objectives are to be achieved in addition to taking into account the objectives that are consistent across the company. Consideration should be given to the company's risk tolerance (Risk Appetite). It should be set up to serve as a guideline for defining company strategies by executives and reviewed by the board of directors to consider the balance between growth, risk and return of the company.

In addition to taking into account the objectives that are consistent across the company consideration should be given to the company's risk tolerance (Risk Appetite). It should be set up to serve as a guideline for defining the company's strategy by management and reviewed by the Board of Directors to consider the balance between growth, risk and return of the company.

Acceptable risks may be quantitative or qualitative. The guidelines are as follows:

- What risks can the company accept what risks are unacceptable to the company.
- What is the risk that needs to be taken in order to achieve the desired return to shareholders and reasonable capital levels.
- The company can accept more risks than is currently acceptable or not if acceptable, how does that risk affect the amount of revenue the company needs.

- What level of capital or income the company can afford to lose if the confidence level is set at a certain level does the company have sufficient funds to support it if a serious risk event actually occurs.
- Are there any risks that the company cannot accept, such as the risk of non-compliance with labor and safety laws in the workplace, etc.
- What risks does the company have to be ready to accept in order to achieve objectives such as reducing profit margins in order to gain higher market share, etc.
- Is it possible for the company to invest in a product with a chance of success low but high yield per product.

Determination of acceptable risk level (Risk Tolerance) is the determination of a deviation from the objective. The operations that are defined under this risk tolerance framework ensure that the management is confident that the company operates within an acceptable risk (Risk Appetite).

3. <u>Event Identification.</u>

Businesses are often subject to uncertainties. The organization cannot be certain whether an event will occur or not or what will the outcome be? In the event identification process management should consider the following:

3.1 All potential risk factors such as strategic, financial, personnel, operations, legal, taxation, work system and environmental risks.

3.2 Sources of internal and external risks.

3.3 Relationship between incidents.

In some cases, potential events should be grouped by incident type and collected all events in the organization that occurs between departments to help management understand the relationship between events and have sufficient information to provide a basis for risk assessment.

Risk Identification is the identification of any event that are likely to occur in the future and have the effect of causing errors, damages, leaks, waste, or adverse events causing the agency's operations to fail to achieve the goals set an event with a negative impact is a risk that needs to be dealt with and events that have a positive impact must be brought back to define the goals or objectives of the company in order to implement and create added value for the company, incident identification can be generated by an individual or a group of individuals such as management and staff involved using a variety of techniques and tools.

Event indication it is the process by which executives and employees work together to identify events or conditions that may affect the objectives of the company by various methods such as:

- Workshops.
- Executive interviews or surveys.
- Comparisons with other companies.
- Employee discussions or internal analysis.
- Guiding events or risk indicators.
- Loss reports such as Loss reports, Accident reports, Plant Incident reports, waste reports and other related reports.
- Analysis of the operation procedure diagram/Operation manual.

The risk identification process should take into account the apparent and vague risks Consideration should be given to broadly covering the following factors:

- External and internal factors that may cause risks.
- Various unfortunate events that may occur such as floods, fires and other natural disasters or ongoing factors such as an inefficient working environment or working too much part-time which these events can result in losses to the company.
- Past events current risks and future trends.
- Causes of events.
- New inventions, new products and new services that the company wants to develop.
- Opportunities from the company's current operations or indication of new activities to add value to the company.

Risk identification techniques methods and tools for the identification of risks are:

1) **Workshop**

Workshops are the most common way of identifying risks. Workshops should be run by a competent coordinator to ensure that the objectives are under the and time things to watch out for is the selection of workshop participants which must be related to the objectives to be discussed each participant must be knowledgeable about the issues to be discussed in the workshop and be able to participate in such discussions.

Workshop participants should possess one of the following qualifications:

- Be involved in the activities to be discussed.
- Be the operator of the activities.
- Be affected by the activities to be discussed.
- Be a supporter and coordinator, e.g. human resource management and information technology department.

The advantage of the workshop is that it allows participants to discuss directly causing honest opinions both accepting each other's opinions including causing controversy on issues of disagreement this will enable the exchange of information widely from many perspectives.

However, the workshop has some limitations which may affect the workshop operation not as effective as it should be the restrictions include.

- Having a centralized culture, However, if the company does not have an open culture, the attendees may not dare to express their opinions or maybe overwhelmed by the attendees of a higher position.
- The ability and experience of the meeting coordinator in the workshop to be more or less efficient or effective depends on the ability and experience the meeting coordinator to encourage participants to express their opinions freely and can coordinate conflicting opinions.
- Time limitation because it is a meeting that must consist of personnel who have the qualifications mentioned above. These are often executives with limited and inconsistent time.

2) Interviews or opinion surveys of executives

Interviews and questionnaires it is a useful technique for collecting risk data information collected from interviews or polls It can serve as an important starting point for discussions in risk workshops.

The advantage of Interviewing or asking for an opinion on risk is the duration this is because interviews can be conducted in different locations and at different times. Therefore, it is suitable for executives who do not have the same time it also allows the interviewees or respondents to express their opinions independently generally, interviews and opinion inquiries risk side will be selected to be used if a private operation is desired.

However, there are some limitations to interviews and risk questionnaires, such as the inability to foster an exchange of opinions it also cannot be carried out in detail like a workshop. Rather, it is often used to collect information from the interviewees or respondents rather than the exchange of information between the people involved. This approach is mainly used to define objectives, scope, risks and controls at the policy or strategic level.

3) Comparison with other companies

Research and comparison with other domestic and international companies may be used to directly identify risks affecting the company.

Research techniques, including the study of related journals attending business-related seminars inquiring about companies involved in Thailand and abroad Internet search asking for opinions in formal and informal discussions with representatives from other companies, research may reveal the following points:

- Infrequent events And it hasn't happened to the company but it is a particular risk for the company. (It has a huge impact)
- The events that have happened or there is a high probability that it will happen in the company and the company has experience in handling such incidents that may occur in the future such as changes of standards relevant to law or computer systems or new technology.
- Best Practice

The limitation of using comparisons with other companies is when considering the experience with other companies may not be accepted if there is an assumption that internal processes and resources are better than other companies or it may not work if such incidents have never happened in the company before.

4) Discussions with employees or internal analysis

Discussions with employees or conducting an in-house analysis for various operating conditions create a source of information and useful events.

5) Leading events or risk indicators

Guiding events or risk indicators able to identify risk factors by tracking information related to an event and enable management to identify current conditions that could trigger future events executives should also consider that are there any indicators of each key risk if risk indicators are not defined management should consider collecting the necessary information for risk indicators to be able to successfully implement risk indicators.

Examples of key risk indicators are:

- Decreased customer satisfaction rate this May indicate a trend of lower future income.
- An increase in overtime wages may indicate an increase in costs or deteriorating quality of work.
- Issuing government consultation reports may indicate future changes in relevant regulations, for example.

Advantages of using risk indicators is able to make a theoretical reference to the source of each risk. However, the quality, accuracy and modernity of risk indicators it is also an important factor that may cause deviations in risk indications. However, the use of risk indicators it is often used to monitor the risks that have already been identified rather than being used to directly indicate risks.

6) Loss reports such as Loss Reports, Accident Reports Waste reports, Plant Incident reports, and other reports related

Studying historical data about income, loss, incidents, or other information about the risk this allows companies to effectively identify risks using quantitative analysis of those data

or analyze differences compared to expected outcomes or budgets to understand the cause or effect of an event. However, the company should not forget to consider both the pros and cons this is because the misunderstanding of the resulting profit can be very risky, as is the understanding of the resulting loss.

The advantage of using a loss event list is the time advantage this can be done with the information contained within the company usually does not show impact cues or the likelihood of an event therefore, users of this risk list should not consider reporting those risk events as a complete risk report.

7) Analysis of the operating procedure diagram

Understanding current operations or best practice processes can help identify risk factors understanding the core processes provides significant benefits to a company's risk management a process diagram may be done in the form of a process map or a description or a combination of both.

The advantage of using operational process diagram analysis is the time advantage this can be done with the information contained within the company usually does not show impact cues or the likelihood of an event or risk factors, so then users of this risk list those risk event reports should not be considered a complete risk report.

Summed up various methods of risk identification as mentioned above there are different advantages and disadvantage sometimes it is popular to take different approaches together, for example, using a questionnaire together with a workshop the use of operational diagram analysis in conjunction with internal discussion and analysis with employees, for example therefore, it should be adjusted to suit the situation and environment of the company.

4. Risk Assessment

This step focuses on assessing the likelihood and impact of an event that may occur on an objective while any event may have a low impact ongoing events can have a high degree of impact on the objectives generally, risk assessment consists of 2 dimensions as follows:

- Likelihood, how likely an event is to occur.
- Impact if an event occurs, how much will the organization be affected.

Risk assessment both qualitative and quantitative assessments can be performed by considering both external and internal events In addition, the risk assessment should be carried out both before the risk management (Inherent Risk) and after the risk has been managed, such as:

- Operations of executives and employees.
- Operational processes.
- Internal control activities.
- Structure and reporting processes.
- Performance measurement and follow-up.
- Communication methods.
- Management's attitudes and approaches to risks.
- Expected organizational behavior and Existing.
- Current Contracts and Partners.

Once the risk has been identified how those risks will affect the achievement of objectives should be assessed management should consider both the risks before control (Inherent Risk) and the risk after control (Residual Risk) by assessing the likelihood and impact by both quantitative and qualitative methods. The outcomes of the risk assessment are as follows:

- An unacceptable risk has been identified.
- Key risks are compared with the company's strategies and policies.
- Actions are selected and prioritized appropriately to reduce the risk.

Likelihood

It is challenging to assess the likelihood of a risk it is generally difficult to find data to support accurate estimates qualitative assessment requires principled and careful analysis where information about failure events or how often past events can be found can indicate the likelihood of future events they can also be used for more accurate mathematical estimations, but in some cases, historical frequencies may not be indicative of future possibilities in that case, appraisers need to use judgment in selecting statistics or future possibilities as inputs for assessment in assessing the likelihood of unclear risk details may cause an assessment error. Therefore, the assessor should consider and improve the details of the risks.

Impact

The risk assessment should take into account both the financial impact, for example, the impact on income and non-financial consequences, for example, rules and regulations customer satisfaction, reputation, personnel, etc. The valuation of the financial impact of a risk is difficult and complex to assess the level of importance of Low-impact and low-impact risk it doesn't need much attention while the risks have a high impact and the likelihood is high need to be considered by senior management promptly.

Level of Risk

Is an indicator used to determine the importance of risk by the level of risk from bringing the likelihood of risks as a basis for risk assessment must be reviewed regularly.

Table 1 Requirements Criteria order of risks

Green Zone			Yellow Zone			Orange Zone			Red Zone		
Number	Chance	Effect	Number	Chance	Effect	Number	Chance	Effect	Number	Chance	Effect
1	1	1	5	3	1	14	4	3	22	4	4
2	2	1	6	4	1	15	5	3	23	5	4
3	1	2	7	5	1	16	1	4	24	4	5
4	2	2	8	3	2	17	2	4	25	5	5
			9	4	2	18	3	4			
			10	5	2	19	1	5			
			11	1	3	20	2	5			
			12	2	3	21	3	5			
			13	3	3						

Rankings 1 through 25 are the ranks used to assess the likelihood of occurrence and impact of the risk as a criterion for risk assessment which must be reviewed regularly.

Guidelines for considering the significance of risks

Assessing the significance of the risks This can be done by referring to the table showing the rank the above risks determining which risks are important to take first in general, a risk sequence may be used for both impact and likelihood and classify groups the importance of risks, for example, the company defines the risks that have impacts and the likelihood of occurring from 22 upwards are important risks that must be considered and managed first, etc.

The determination of the significance of the risks of the company should be considered by senior management and approved by the risk management committee determining the company's risk significance this can be illustrated in the figure below, where the X-axis represents the potential risk exposure and the Y-axis showing potential effects The priorities of the risks were determined from 1-5 levels if the value is low, it means the risk is very low and the higher the value , the higher the risk by definition of each level of risk show as picture and table.

Table 2 **Organizational Risk Assessment Table (Risk Assessment Metrix**

Risk Assessment			The possibility of exposure to the organization				
Impact/violence on the organization	Very High	5	19	20	21	24	25
	High	4	16	17	18	22	23
	Moderate	3	11	12	13	14	15
	Low	2	3	4	8	9	10
	Very Low	1	1	2	5	6	7
			1	**2**	**3**	**4**	**5**
			Very Low	Low	Moderate	High	Very High
			Chance				

Valued assessed based on the likelihood of occurrence and impact	Risk Level	Things to do
22-25	Very High	Unacceptable level it is necessary to expedite the risk management to an acceptable level immediately.
14-21	High	Unacceptable level the risk must be managed to keep it at an acceptable level.
5-13	Moderate	Acceptable level but there must be controls to prevent risks from moving to unacceptable levels.
1-4	Low	Acceptable level without control no additional management is required.

From the picture above indicates the extent of the significant risk, i.e. the risk value of the level effects and chances of occurrence from 22 upwards.

The score in each box arises from considering the level of risk both likelihood and impact by weighting the impact more than the likelihood, for example, the risk assessment in case of likelihood is 4, the impact is 5, the risk is 24, which means that it is a very important risk,

Once the risk level has been reached the risk should be taken at a very serious level can cause a lot of damage, and a high chance of occurrence let's speed up the deal before other things. As for the non-severe risks, there is a low probability of occurrence it is classified as a risk that does not require any action in the case of budget manpower or time constraints prioritizing risks allows for planning and allocating of resources correctly by selecting the available risk metrics more severe and more frequent risks go to less severe and frequent opportunities.

Table 3 Organizational Opportunity Assessment Table (Risk Assessment Metrix)

Risk Assessment			The possibility of an opportunity for the organization				
Positive impact on the organization	Very High	5	19	20	21	24	25
	High	4	16	17	18	22	23
	Moderate	3	11	12	13	14	15
	Low	2	3	4	8	9	10
	Very Low	1	1	2	5	6	7
			1	2	3	4	5
			Very Low	Low	Moderate	High	Very High
			Chance				

Values assessed based on the likelihood of occurrence and impact.	Risk Level	Things to do
22-25	Very High	The business opportunity is very high.
14-21	High	The business opportunity is high.
5-13	Moderate	The business opportunity is very moderate.
1-4	Low	The business opportunity is very low.

When the opportunity level is good for the organization it should bring a low positive impact can cause low business opportunities let's speed up the deal before other things the positive impact is high can cause the business opportunity is very high be dealt with in the next order.

Therefore, risk is a danger or possibility that something is dangerous or not desirable will occur in general, the risk versus opportunity (opportunity) is often viewed as a counterpart and should be in a state of balance as much as possible it is expected that the results will bring more benefits than harm , Therefore, the main objective of risk management thereby reducing the risks that may occur to a minimum and maximizing the opportunities that may arise for the operations of the organization.

5. Risk Response or Risk Management

It is an assessment of the control activities that should be carried out or that already exist that can help control risks or risk factors are sufficient or not or how effective the control objectives are, considering the costs and benefits incurred risk management is a strategy or activity set for manage risks by reducing the likelihood and impact of risks in accordance with the company's acceptable risk level.

When considering risk management, costs and benefits must be taken into account by using either strategy or all such as:

1) **Risk Avoidance** is the management of risks that are very high and the agency is unacceptable therefore decided to cancel that project/activity. However, if using this strategy, it may be necessary to consider whether the objectives can be achieved or not to make further adjustments.

2) **Reduction/control of risks (Risk Reduction)** is the improvement of working systems or designing new working methods to reduce the likelihood of or reduce the impact of risks to an acceptable level.

3) **Diversification of risks or the transfer of risks (risk sharing)** is the distribution or transfer of risks to other people or companies to help share the responsibility in order to reduce the likelihood and impact of risks to an acceptable level.

4) **Risk Acceptance** the remaining risks at present are at acceptable levels without taking any action to reduce the likelihood of repercussions that may occur it is often used for the risk that the high cost of management measures is not worth the benefits.

Factors in determining risk management strategies are as follows:

- **Impact Assessment and Chance from the implementation of risk management strategies** to assess the choice of each risk management strategy executives must understand that risk management activities can affect the impact and the likelihood of different risks for example, buying forward foreign exchange rates it is an activity that can reduce the impact of exchange rate fluctuations. However, this cannot reduce the likelihood of exchange rate fluctuations on the other hand, choosing to purchase more domestic raw materials can reduce the likelihood of changes in foreign exchange rates but unable to mitigate the potential impacts, etc. Therefore, the assessment of the impact and the likelihood of risks that may change from the implementation of risk management activities, therefore, it should be considered before deciding on a strategy so that the risk level is consistent with the acceptable risk level of the company.

- **Assessment of costs and rewards of implementing risk management strategies** because the company's resources are limited therefore, it is necessary to assess the cost and the return incurred costs can generally be quantitatively calculated by calculating direct and indirect costs. It can also be considered in terms of the time and resources used to implement such risk management strategies. For the consideration of compensation, it can be assessed in terms of the benefits that will be obtained for the achievement of the relevant objectives.

If the risk management activities are carried out if the return from the operation is not worth the incremental cost management may consider a risk transfer approach (Sharing) to distribute costs to outside agencies, such as insurance or joint ventures, etc. Management may choose one of the risk management methods or a combination of methods to manage the risk to the desired level.

6. Control Activities Control

Activities are the policy and operating process to ensure that risks are managed because each organization has its own specific objectives and techniques for implementation. Therefore, the control activities are different. Controls reflect the organization's internal environment, business nature, structure, and culture and if the operation uses information technology systems it is necessary to consider general controls in information technology systems and controls for each work system.

Types of Control Activities

1) **Preventive** controls actions or pre-arranged controls to reduce the likelihood of negative outcomes/effects such as:
   - Segregation of duties
   - Password use
   - Training
2) **Detective** controls, actions or controls to find the cause when errors or irregularities have already occurred, such as:
   - Review reports
   - Confirmation
   - Asset counting
   - Error reports
3) **Corrective control (Corrective)** action or control to correct the damage or reduce the damage caused by mistakes or irregularities such as account reconciliation.
4) **Directive**, action, or control that promotes or stimulates to achieve of the desired objectives, such as rewarding those who perform well control activities assure management that risk management activities are carried out appropriately and promptly in some cases, one control activity may involve multiple risk management activities on the contrary one risk management activity may involve several control activities and in some risk management strategies and control activities may be the same activity.

Control activities are an important process for management in achieving the company's objectives as each company has its own set of objectives and implementation techniques are company-specific, therefore control activities are different control reflects the environment, nature of business, and internal structure company background and culture.

After an initial roadmap for risk management has been formulated, and when the initial plans have been approved there should be an action plan which defines the responsible persons and those involved to implement them and inform the responsible person and those involved in it so that they can implement by specifying the time for completion this ensures that the strategy is implemented to achieve the expected opportunities.

In general, a risk-taker is a person who has direct responsibility for the work and has sufficient decision-making power to make the action plan for risk management success where an action plan has more than one responsible party and contributor those responsible for risk will play a role in coordinating with the contributing parties to ensure timely and effective implementation of risk management measures after the action plan has been approved and approved the person responsible for the risk is responsible for the implementation of the action plan and follow up on the performance of the action plan in addition, the risk management team must report the status of progress or problems of the action plan for further reporting to the company's risk management committee the company's risk management committee may request that those responsible for risk directly report the status and progress of the action plan.

After completing the implementation of the action plan those responsible for risk should consider factors such as changes in the business environment that are associated with risks existing risk control and the effectiveness of the implemented action plan, etc., and assessing the level of risk based on the likelihood and impact assessment criteria the person responsible for the risk will be required to present the reassessed level of risk and evidence supporting the said risk level to the risk management committee for further approval.

Control activities for information technology systems can be grouped into two categories: general control, and general control and specific control system the general control covers the infrastructure and management of information technology security administration

purchasing a ready-made program development and maintenance system-specific controls are designed to ensure the integrity of the recorded and processed data true and real.

7. Information and Communication

Is essential for organizations to identify, assess and manage risks Information relating to the company from both external and internal sources it should be recorded and communicated appropriately in form and time to help relevant personnel to respond quickly and efficiently to incidents.

Risk reporting

This is to report the effectiveness of all risk management processes carried out sequentially to management and approve the implementation of the risk management plan.

Benefits of the Risk Task List These are as follows:

- Assure the Board of Directors that the Company's risks are consistent with the approved risk strategy and consider that risk management duties are being carried out effectively.
- Top management can identify and understand the risks that arise and determine effective risk mitigation activities at the strategic and operational levels.
- Executives of various departments it can confirm that the controls related to major risks have been implemented and implemented successfully and the resulting errors are properly reported.

8. Monitoring and review (Monitoring)

Is an activity used to monitor and improve risk management activities to ensure that risk management measures are implemented generally, risk monitoring activities are routine activities on an ongoing basis but in some cases, it can be a specific activity the objectives of risk monitoring and risk management include:

- Ensuring that those risks are managed as planned.
- Assessing the effectiveness of risk management plans and activities.
- Reconsideration of new risks when the situation arises change.

Follow-up is typically performed by internal company personnel it helps to monitor risk management from time to time risks and risk management are subject to change over time once effective risk management can turn into inappropriate activity could the control activities be less effective should continue or there may be changes in objectives or processes. Therefore, management should regularly assess risk management processes to ensure that risk management is always effective risk monitoring and reporting are most effective when linked as part of the company's normal operating and reporting processes.

Companies should encourage proactive and consistent two-way communication formal communication channels used to determine risks controls and action plans include general meetings of executives working group meeting executive monthly report risk management committee meetings, etc. continuous communication will provide sufficient risk information and be presented for timely decision-making in some cases, the risk is dealt with in an expedited manner by talking on the phone or the preparation of specific incident reports it may be more appropriate to wait for an official report.

Risk Management Terminology

Vocabulary	Description
Iternal Control	Processes carried out by the Board of Directors, executives and other personnel to ensure to a certain extent that the objectives can be achieved.
Monitoring	Strict inspection and supervision or record of the progress of activities, operations or systems on a regular basis to identify changes that have occurred.
Risk Response	Selection and application of appropriate risk management options.
Risk Identification	The process of considering events that may occur and have a negative effect on company objectives which must consider the cause or origin of the take that risk.
Risk Management	Risk management is a process, culture, and structure that affect the Board of Directors executives and employees to formulate strategies throughout the company It is designed to identify events that may affect the Company and to manage risks within acceptable risks and to use measures to enable companies to achieve their goals. objective.
Risk Assessment	The overall process of analyzing and prioritizing risks.
Reasonable Assurance	The concept of risk management is that No matter how well the company is designed or operated cannot guarantee that it will be achieved all objectives of the company due to existing limitations which cannot be managed in the risk management system.
Frequency	A measure of the incidence rate, which describes in terms of the number of incidents occurring in a given time period.
Probability	The likelihood of an event or any outcome, a measurable outcome as the proportion of the number of events or results to the total number of events or outcomes that may occur. Probability ranges between 0-1, where 0 indicates an event or outcome that will never occur and 1 indicates an event or outcome that will definitely occur.

Vocabulary	Description
Uncertainty	The inability to predict the future with certainty the likelihood and impact of such events.
Loss	Financial results or the consequences that occur in the negative.
Cost	The cost of both direct and indirect activities includes money labor time and non-monetary losses.
Inherent Risk	Risks affecting the company existed before the management had to take any action.
Risk Appetite	A mention of risks or the overall types of risks that the Board of Directors and management are willing to accept to carry out the mission or vision of the company, strategies and policies. that is approved by the board and management It shows the readiness for that level of risk.
Risk Tolerance	Deviation or variation from level the goals set by the executive committee and executives are ready to accept such risks related to the strategy or objectives of the company.
Residual Risk	The level of risk remaining after the risk has been managed to reduce the likelihood or impact of the risk.
Risk Owner	A person or group responsible for cutting decide on a risk management plan or action plan that is appropriate for unacceptable risks.
Stakeholders	Persons or companies that have an impact on or were affected by or understand that one will be affected by decisions and activities.
Event	What happened from within or outside and affected the company which happened somewhere during a particular period of time.
Likelihood	Quantitative description of risk with probability and frequency.
Accept	The risk after control is at an acceptable level without any further action that affects the likelihood or effect of the risk.
Reduction	Additional actions to reduce the likelihood of or the impact of the risk to an acceptable level.
Avoidance	Actions to cancel or avoid activities that pose a risk can be achieved or not to make further adjustments.
Sharing	The transfer or sharing of certain risks with another person or company.
Sharing	The transfer or sharing of certain risks with another person or company.

The Risk Management Working Group of Muangthai Capital Public Company Limited

Consists of the Company's various departments as follows:

No	Department	Main responsible person
1	Branch Affairs Department	Mr. Surapong Pechaumpai
2	Debt Department	Ms. Duangkhae Songnuy
3	Accounting Department (Preparing Financial Statements)	Mr. Surat Chayavoradech
4	Accounting Department (Branch Coordinator)	Ms. Vimonrat Nujul
5	Finance Department	Mrs. Pranee Suyapol
6	Treasury Department	Mr. Kitsada Kuruchitkosol
7	Department of Information Technology (Programmer)	Mr. Aswin Kruawan
8	Department of Information Technology (IT Support)	Mr. Wirot Loythuplert
9	Human Resources Department	Mr. Worawat Kanchanakul
10	Purchasing Department	Mr. Channarong Chiangnoon
11	Admin Department	Ms. Renu Pomsomboon
12	Marketing	Ms. Sirilak Srimanee
13	Project for the construction of a new head office building	Mr. Amornthep Pookang