Enterprise Risk Management Manual

Table of content

Part 1: Enterprise Risk Management Policy

1.1 Objective

Nowadays, businesses face uncertainties from both internal and external factors, thus giving rise to both opportunity and risk. An opportunity has the potential to enhance the organisation's value while risk can adversely affect both the financial and non-financial value of the business. So, Enterprise Risk Management (ERM) is an important tool to help maintain and promote the organisation's goals and objectives, as well as preventing any uncertainty or risk and by doing so, help to reduce the potential for loss. In addition, ERM is a significant element of good corporate governance, with a focus on transparency, efficiency, and a positive brand image. Also, it creates both short and long term value for organisations under the management of the Board of Directors, Executive Committee, management and all employees.

1.2 Scope

This policy applies to the Board of Directors, Executive Committee, management and all employees. The policy's objective is to ensure that risk management is consistent with strategy, action plans, and project scenarios, and to enhance the understanding of the purpose, authority, roles and responsibilities of the organisation, and corporate risk management reporting within it.

1.3 Definition of terms and types of risk

1.3.1 Definition of terms

Business unit/Departmental risk is the risk that may arise from the operation of each department, unit or project. The risk can be managed by the department, unit or project or controlled by an existing internal control activity.

Control activity is a policy or measure employed by the management that helps to make sure that its response to the control is carried out and the risks identified are reduced to achieve the objectives of the organisation.

COSO (The Committee of Sponsoring Organisation of the Treadway Commission) is a joint initiative of the five private sector organisations listed below, which is committed to developing the integrated frameworks of enterprise risk management and internal control.

1. American Accounting Association
2. American Institution of Certified Public Accountants
3. Financial Executives International
4. The Institute of Management Accountants
5. The Institute of Internal Auditors

Corrective controls are designed to correct errors or risks, or reduce the impact from negative events and errors.

Detective controls are a control mechanism that find problems in a company's processes to enable proper corrective measures.

Enterprise Risk Management are culture, capabilities, and practices integrated with strategy-setting and their performance, which organisations rely on to manage risk that might affect the corporate value.

This process, put into practice by the Board of Management and all personnel in the company, is applied within a strategic setting and operations across the enterprise. It's designed to identify potential events that may affect the organisation, and manage risks so as to be within its risk appetite, which would help the organisation attain reasonable assurance that it can achieve the organisation's objectives.

Impact is the result or effect of a risk that might cause a range of possible types of impact. The impact of a risk may be positive or negative relative to the entity's strategy or business objectives, including: the financial impact, reputational impact, and regulation and compliance impact.

Inherent risk is an existing risk of the organisation without any activity to reduce the likelihood and impact.

Internal control is a process, put into effect by an entity's Board of Directors, management, and other personnel, which is designed to provide reasonable assurance regarding the achievement of objectives relating to the following:

- Effectiveness and efficiency of the operation
- Reliability of the financial report
- Compliance with related laws and regulations

Likelihood is the possibility that a risk will occur based on the probability of occurrences or the frequency of events.

Monitoring is the process of regularly reviewing, observing, and recording progress, the control activity or system to locate changes.

Preventive controls are used to keep a loss or an error from occurring.

Reasonable assurance is an acknowledgment that regardless of the good design of the risk management system, the achievement of the organisation's goals can't be guaranteed due to the limitations of the risk management of the organisation.

Residual risk is an amount of risk or danger associated with an action or event remaining after natural or inherent risks have been reduced by risk controls in order to improve the likelihood and impact of the risk.

Risk is an uncertain event or condition that threatens an organisation's objectives and causes a negative impact on the organisation in terms of both financial and brand reputations.

Risk appetite is a type and amount of risk, on a broad level, an organisation is willing to accept in pursuit of value.

Risk assessment is the identification, evaluation, and estimation of the levels of risk involved in a situation to prioritise risks.

Risk factor is a root cause which can determine the proper risk response measure. Risk factors are determined by internal and external factors such as corporate regulations, work processes, the economy, society, politics, customers, competitors, etc.

Risk identification is the process of determining risks that could potentially prevent the organisation from achieving its objectives by considering what, why, and how.

Risk map is a data visualisation tool for communicating the specific risks an organisation faces as well as risk assessment results, showing the likelihood and the impact of an occurrence.

Risk owner is a person who is ultimately accountable for prescribing the risk management plan to ensure the risk is managed to achieve the objectives according to the time frame, monitoring the plan implementation progress and reporting the events to the Risk Management and Risk Management Committee. Also, risk owners are the ones who are significantly affected by the risk, or are directly associated with the risk.

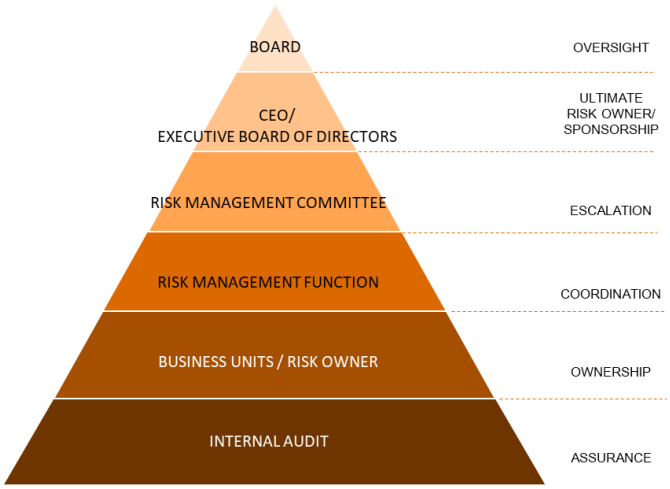
Risk register is a tool for documenting risks, and actions to manage each risk, and to fulfill regulatory compliance acting as a repository for all risks identified, which includes additional information about each risk, e.g. objectives, nature of the risk, reference and owner, risk details, current mitigation measures, risk assessment results, risk management plans, responsible persons, and deadlines.

Risk Response is a risk management measure, which can be classified into the following categories:
(1) Accept

(2) Avoid
(3) Pursue
(4) Reduce
(5) Share

Stakeholders are parties that are affected by the organisation's operations e.g. shareholders, community, employees, customers, and salespeople.

1.4 Roles and responsibilities



Risk Management Structure

Board of Directors

- Overseeing and approving the risk management framework and risk appetite.
- Supervising the processes of risk management and internal control to ensure the processes are effective.
- Reviewing risk reports from the Risk Management Committee and maybe providing additional comments, if any, on the risk management plan or identifying additional significant risks to the organisation.
- Establishing a risk aware culture throughout the enterprise.

Audit Committee

- Approving an internal audit plan using risk information as reported by the Risk Management Committee.
- Supervising internal auditors to review the risk management process and internal controls to ensure that the process is efficient and effective.
- Promoting a corporate culture of risk management.

CEO/Executive Board of Directors

- Showing good intentions as an example to employees. Encouraging the corporate culture of risk management and working to ensure effective and continuous risk management.
- Encouraging the continuous identification, evaluation, management, and reporting of risks as a part of normal operations.
- Defining the roles and responsibilities for managing the risks with the management.
- Reviewing performance measures against the risk appetite and providing advice on corrective actions, as well as identifying additional significant risks to the organisation.

Risk Management Committee

- Reviewing and approving the risk management policy.
- Supervising the implementation of the risk management framework and risk management policies.
- Supervising risk management to ensure it complies with the risk appetite.
- Receiving key risk reports from the Risk Management Department and providing additional comments, if any, on the risk management plan, as well as identifying the additional significant risks to the organisation.
- Promoting awareness of risk in the organisation.
- Reporting corporate risk to the Board of Directors.

Management

- Complying with policies and the risk management framework and communicating with employees within the department to improve their understanding and awareness of the importance of risk management.
- Identifying, evaluating, managing and monitoring risks associated with responsibilities.
- Providing good internal controls to ensure that risk is properly managed according to the risk appetite.
- Reviewing and approving the risk report of the responsible department before reporting to the Risk Management Department.
- Promoting a culture of risk management. Employees should be aware of the risks involved when making important decisions and in every process to achieve business objectives.

Risk Management Department

- Preparing and reviewing the risk management framework and processes (i.e. risk management policies, risk service structure, risk appetite level, and risk management manual) in accordance with the company's operations and good practice.
- Developing risk management tools and procedures to identify, assess, monitor and report risks consistently across the organisation, including investment projects.
- Communicating and advising the Risk Management Committee, the management, and employees of the Company regarding the organisation's risk management framework and procedures to enhance their knowledge and understanding.
- Helping to arrange risk workshops to support the identification, assessment and preparation of a risk management plan for each department in order to conform to the practices of the organisation.
- Collecting and analysing risk data to prepare an enterprise risk register and coordinating the exchange of risk information between departments. So, the risk owner can complete the risk management plan as he or she is responsible.
- Monitoring and reviewing the work progress according to the risk mitigation plan and risk indicator to report to the Risk Management Committee.
- Responsible for the risk information for internal departments and external organisations such as preparing risk factors in the annual report, providing a risk analysis for internal audit plans, and preparing risk reports to report to the Risk Management Committee and the Board of Directors.
- Promoting a culture of risk management across the organisation.

Internal audit

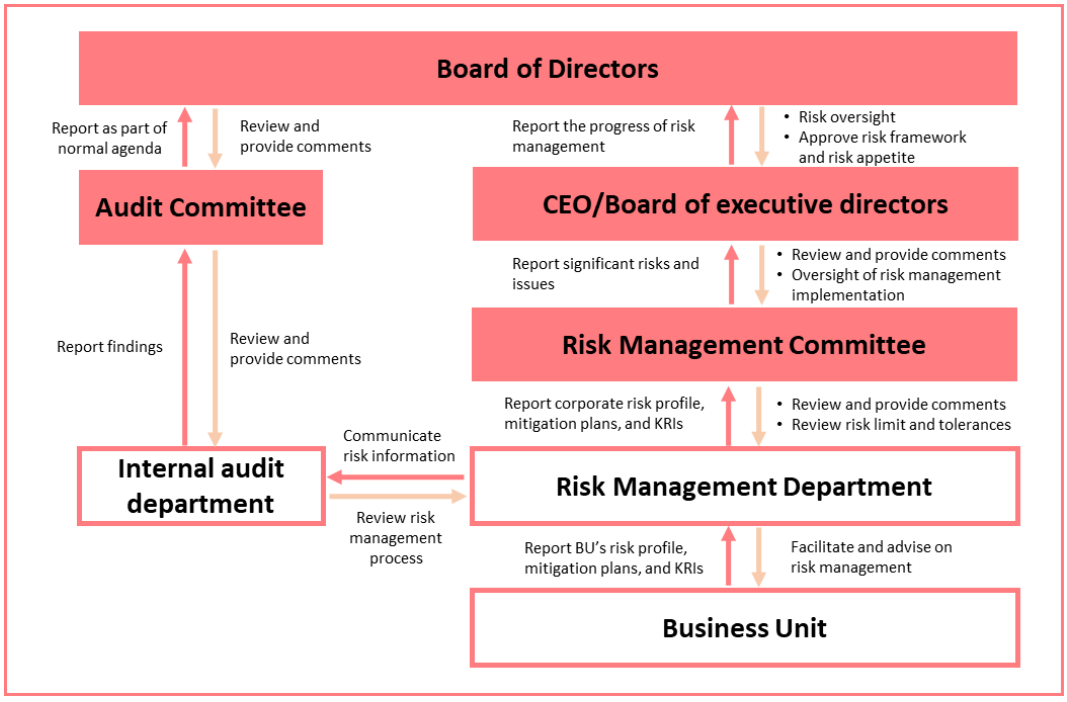
- Communicating with the Risk Management Department to take risks into consideration for audit plans and performing internal audits.
- Reviewing the compliance with policy and risk management processes to ensure that they are implemented properly, and reporting the result to the Audit Committee.
- Share concerned issues and risks found with Risk Management team in order to ensure that all concerned risks are listed in the Risk Register with appropriate mitigation plans.

Staff

- Ensuring that risk management and internal control are a part of daily operations and complying with the policy, framework, and risk management process approved by the Board of Directors.
- Reporting any major risk or problem in risk management to the supervisor.

1.5 Components of enterprise risk management

The organisation's risk management framework is designed so that risk is identified, assessed, managed, monitored, and reported continuously throughout the organisation. The Risk Management Department should report the risk and risk monitoring results to the Risk Management Committee at least every quarter and report to the Executive Board, The Audit Committee, and the Board of Directors at least once per year.



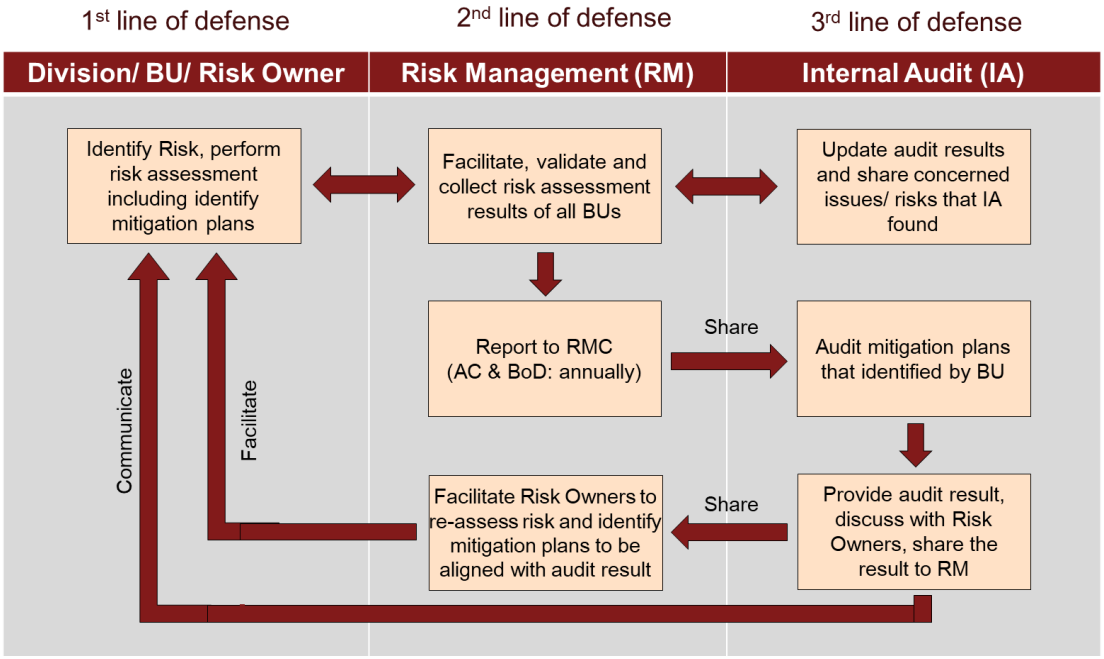
1.6 Linkage between Risk Management and Internal Audit

The model below shows the linkage between Risk owner, Risk Management and Internal Audit in Three Lines of Defense Model which addresses how specific duties related to risk and control could be assigned and coordinated within the organization. In order to assure that all significant risks are addressed appropriately, careful coordination is necessary to avoid unnecessary duplication of efforts. The Model clarifies the difference and relationship between the organizations' assurance and other monitoring activities; activities which can be misunderstood if not clearly defined.

The responsibilities of each of the groups (or "lines") are:

1. Own and manage risk and control (Division/BU/Risk Owner).
2. Facilitate risk and control, consult, communicate in support of management and Risk Management Committee (Risk Management).
3. Provide independent assurance the effectiveness of management of risk and control. Also, updating and communicating audit results to 1st Line and sharing concerned issues and risks found with Risk Management team (Internal Audit).

Each line has its own unique roles and responsibilities. They are separate lines but should not operate in silos. They should share information and coordinate efforts regarding risk, control and governance.


1st line of defense
2nd line of defense
3rd line of defense
Division/ BU/ Risk Owner
Risk Management (RM)
Internal Audit (IA)
Identify Risk, perform risk assessment including identify mitigation plans
Facilitate, validate and collect risk assessment results of all BUs
Update audit results and share concerned issues/ risks that IA found
Report to RMC (AC & BoD: annually)
Share
Audit mitigation plans that identified by BU
Communicate
Facilitate
Facilitate Risk Owners to re-assess risk and identify mitigation plans to be aligned with audit result
Share
Provide audit result, discuss with Risk Owners, share the result to RM

Part 2 : Risk Management Framework and Processes

2.1 Risk management framework

Enterprise Risk Management—integrated with strategy and performance to clarify the importance of enterprise risk management in strategic planning throughout an organisation— has been adopted in accordance with The Committee of Sponsoring Organisations of the Treadway Commission (COSO). This is to prevent risk impact and to align the strategy and performance across all departments and functions. The framework itself is a set of principles organised into five interrelated components:

Source: COSO Enterprise Risk Management: Integrating with Strategy and Performance

2.1.1 Governance and Culture

Governance sets the organisation's tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management. Culture pertains to ethical values, desired behaviours, and understanding the risk in the entity.

1) The organisation defines the desired behaviours that characterise the entity's desired culture.
2) The Board of Directors oversees the strategy and carries out governance responsibilities to support management in achieving strategy and business objectives.
3) The organisation is committed to building human capital in alignment with the strategy and business objectives.
4) The organisation demonstrates a commitment to the entity's core values.
5) The organisation establishes operating structures in the pursuit of strategy and business objectives.

2.1.2 Strategy and Objective-Setting

Defining the clear objectives is the first and foremost step for the risk management scheme. By doing so, the organisation is required to establish the objectives and goals of business operations for the organisational levels e.g. vision, mission, strategy and policy. For the operational level, the objectives include, for example, goals and operation plans. The objective-setting work should be performed prior to the risk identification process. In addition, the business objectives should be aligned with strategic planning and risk appetite, and recorded in writing and communicated to all staff levels throughout the organisation. The business objective setting should be based on the following:

1. Strategy associated with corporate objectives and missions.
2. Business performance concerning the efficiency and effectiveness of the operations and profitability.
3. Risk report (internal and external).
4. Compliance with law, rules, and regulations.

2.1.3 Performance

Risks that may affect the achievement of the strategy and business objectives need to be identified and assessed. Risks are prioritised by severity in the context of risk appetite. The organisation then selects risk responses and takes a portfolio view of the amount of risk it has assumed.

2.1.4 Review and Revision

By reviewing the entity's performance, an organisation can consider how well the enterprise risk management components are functioning over time and in light of substantial changes, and what revisions are needed.

2.1.5 Information, Communication, and Reporting

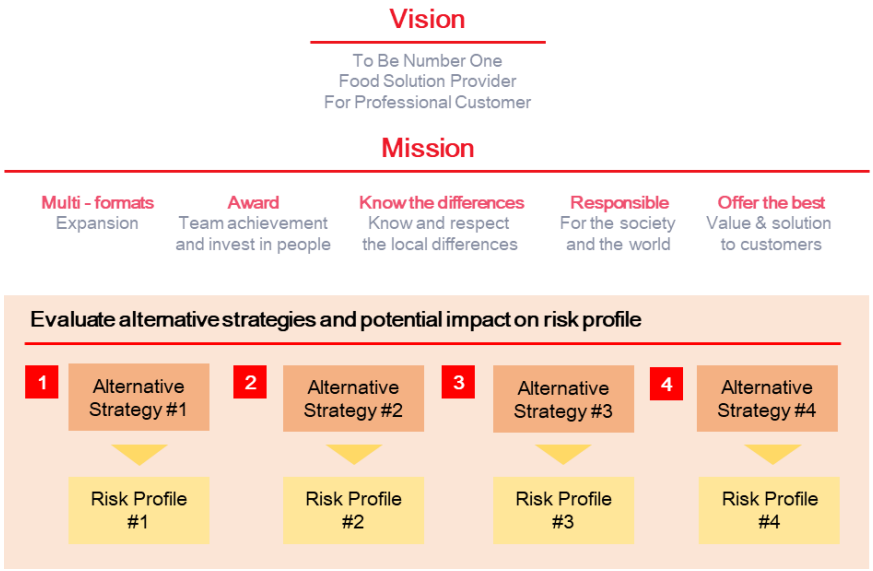
The organisation needs to set up an efficient information and communication system to support risk management and align with the defined risk management framework and processes. To achieve efficient risk management, necessary information from both internal and external sources, are required to be communicated in a proper, timely manner. Specifically, the information related to risk identification, assessment, and management should be shared throughout the organisation, thus encouraging the organisation to manage risk efficiently and effectively.

2.2 Enterprise risk management process and implementation

2.2.1 Strategy and Objective-Setting

Process	Description
1) Analysing business context	An organisation considers business context when developing strategy to support its mission, vision, and core values, which covers both the external and internal environment. • The external environment is part of the business context. It is the uncontrollable factor outside the entity that can influence the entity's ability to achieve its strategy and business objectives. For example: o Culture, politics, laws, regulations, finance, technology, economy, and a domestic and international competitive environment. o Main drivers and trends that affect the objectives of the organisation. o The recognition and value of stakeholders outside the organisation. • An entity's internal environment is the controllable and changeable factor inside the entity that can affect its ability to achieve its strategy and business objectives. For example: o Competency of the organisation in terms of resources and knowledge such as capital, time, personnel, processes, systems and technologies. o Information systems, communication, formal and informal decision-making processes. o Stakeholders within the organisation. o Policy, objectives and corporate strategy. o The recognition of value and organisational culture. o Organisational structure such as management system and roles and responsibilities.

Process	Description
2) **Defining risk appetite**	The operations of the company shall include the risk to be a barrier that makes it impossible to achieve the objectives or goals of the Company as defined. If the risk is at a certain level, and the company can continue to achieve its objectives, the risk level is called 'Risk Appetite', which should be set by the Executive Board or Executive and approved by the Board of Directors. It is regularly monitored to ensure that it complies with the company's vision, mission, strategies, or policies, which are changeable. The factors that should be considered in determining risk appetite are: • Strategies, goals, vision and mission of the company. • External factors such as uncertainty of the business environment and the change in the selling price of products or raw materials. • Internal factors such as operational risk and changes in organisational structure Therefore, the level of risk appetite under the risk assessment criteria and risk map can be defined as follows: 1. The acceptable level of risk is where the risk is assessed to be at a low level but needs to be controlled so that the risk won't be moved to a level beyond the risk appetite. 2. The level of risk that exceeds the acceptable level of risk is the risk assessed as material and significant. For example: • The company doesn't accept risk for financial reports that are unreliable, and don't comply with accounting standards. • The company doesn't accept the risk of net profit below the target of 10%. • The company doesn't accept the risk of non-compliance with the law, resulting in the company being guilty of misconduct. • The company doesn't accept the risk of adverse news about products and a negative reputation without corrective action within 24 hours. • The company doesn't accept the risk of critical business interruption that takes more than 24 hours to recover from. • The company doesn't accept the risk of the turnover rate for staff levels ..... exceeding ..... percent. • The company doesn't accept the risk of serious injury to customers and employees. • The company doesn't accept the risk of net loss exceeding .....

Process	Description
3) **Aligning the risk management with the strategy**	An organisation must evaluate alternative strategies as part of strategy-setting and assess the risk and opportunities of each option. An effective strategy must support the mission and vision and align with the entity's core values and risk appetite. If it doesn't, the entity may not achieve its mission and vision. A part of enterprise risk management includes evaluating strategies from two different perspectives: 1. The possibility that the strategy doesn't align with the mission, vision, and core values of the entity, and 2. The implications from the chosen strategy. The organisation seeks to identify and understand the potential risks and opportunities of each strategy being considered. The management and the Board use these risk profiles when deciding on the best strategy to adopt, given the entity's risk appetite. This practice will enable the organisation to define its objectives that accord with the strategy and resources allocation.  The organisation should expect that the strategy it selects can be carried out within the entity's risk appetite. That is, the strategy must align with the risk appetite. Also, the risk and opportunity resulting from each strategy should be taken into consideration.

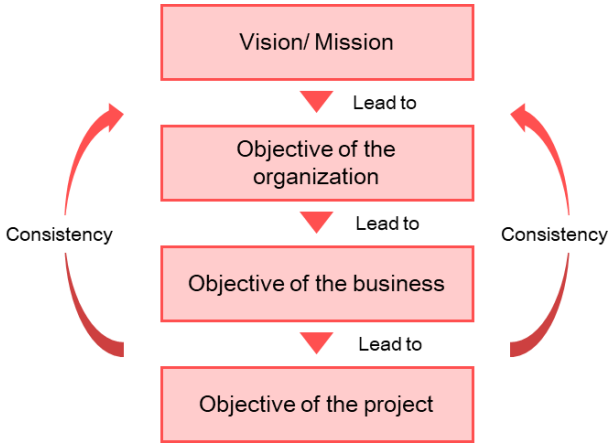
<table>
<tr><th>Process</th><th>Description</th></tr>
<tr><td>4) Formulating business objectives</td><td>

The organisation considers risk while establishing the business objectives at various levels that align and support strategy.

Business objectives may cascade throughout the entity (divisions, operating units, functions) or be applied selectively. Cascading objectives become more detailed as they are applied progressively from the top of the entity down. Objectives at different levels should align with the strategic plan and risk appetite defined by the organisation. The consistency will lead the organisation to achieve its mission and vision. For example, business objectives may relate to:

- strategy involving corporate goals and mission
- operations involving performance and profitability
- reporting (internal and external)
- compliance with laws and regulations

Objectives at different levels



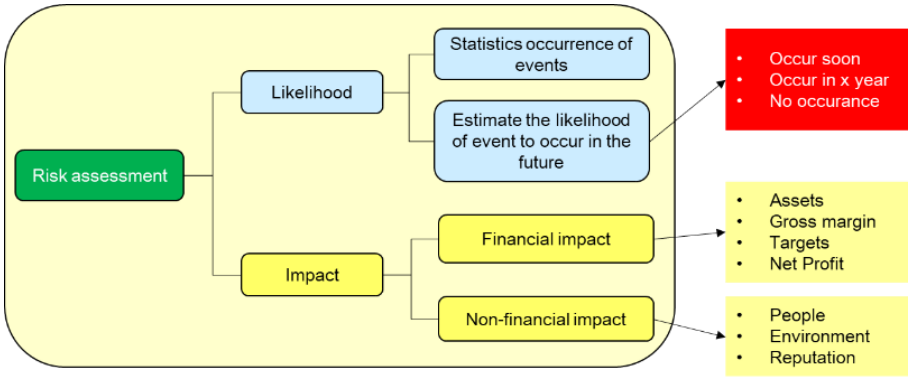
Establishing business objectives (SMART objectives)

The organisation develops business objectives that are specific, measurable or observable, achievable, relevant, and time bound.

Specific	Objectives should be clear in order to achieve a consistent understanding of desired outcomes.
Measurable	Objectives should be measurable. It should also specify the criteria and the information to be used for the measurement.
Achievable	The objective or goal must be reasonable and achievable based on factors such as market conditions, time frame, resource allocation, etc.
Relevant	Returns or results of the established objectives must be consistent and supportive to achieve objectives at the same level and the level above.
Time bound	The time frame should be clearly defined.

</td></tr>
</table>

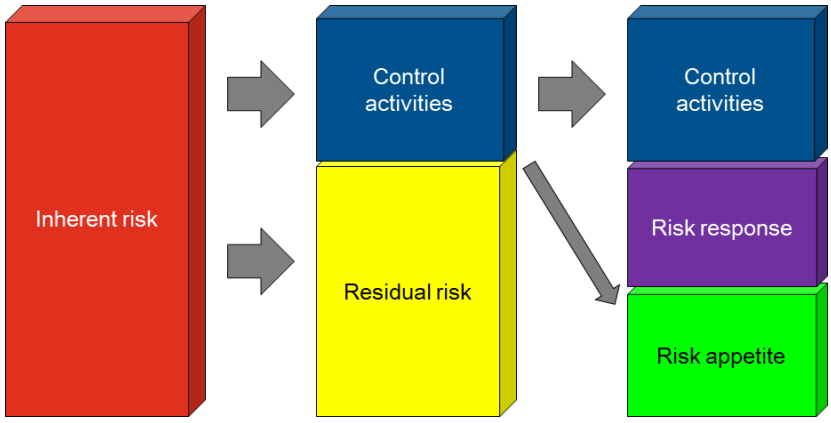
2.2.2 Performance

Process	Description
1) **Risk identification**	Considering the causes and sources of risk, for both a positive and negative impact, and the likelihood of such events and their effects.  **1.3.2 Type of risks**  The eight risks are classified as follows: 1. **Strategic risk:** Caused by a change in the business environment which affects the goals or long-term plans such as the volatility of oil prices, changes in state policy, and economic conditions. 2. **Operational risk**: Caused by a change in the working environment which has an impact on work processes and capabilities in daily practice such as accident or hazards, as well as the risks associated with information technology and knowledge that help achieve the goals. 3. **Financial risk**: Caused by a change in economic and financial conditions, resulting from external factors such as exchange rate fluctuations, interest rates, etc., or from internal factors such as liquidity management, credit, investment, etc.

<table>
<tr><th>Process</th><th>Description</th></tr>
<tr><td></td><td>
4. Compliance risk: Caused by non-compliance with laws and regulations such as the regulations of the Stock Exchange of Thailand, including the risks associated with the law in business operations.
5. Reputational risk: Caused by actions that have an impact on corporate image and corporate reputation such as complaints about product quality or the disapproval of the community.
6. Environmental risk: Caused by natural factors e.g. climate change, flood, fire, and earthquake. These events may affect plants or buildings such as creating an inability to distribute products to branches or the loss of human resources.
7. Economic risk: Caused by economic changes that will affect the organisation such as the economic crisis, fluctuations in the cost of products, interest rate, inflation, foreign exchange rates, etc.
8. Social risk: caused by events such as human rights abuses, terrorism, and demographic change. This will affect the demand for products and services and create a lack of human resources and productivity.

Tools for identifying risks
Risk identification should be performed by the management and the process owner. Examples of techniques and tools that help identify the risks are:
<table>
<tr><td>Workshop</td><td>The workshop should be conducted by a qualified facilitator. The participants must be involved in the objectives or have knowledge of issues or processes to be discussed.</td></tr>
<tr><td>Interview or survey</td><td>Sometimes the process owner may disregard their own risk. So, listening to the opinions of others is another way that helps identify more comprehensive risks. Interviews and surveys are useful techniques for collecting risk data. It’s a good starting point for discussion in risk workshops.</td></tr>
<tr><td>Benchmarking</td><td>Researching and benchmarking with other organisations both locally and internationally may help the company identify more risks. This is done by, for example, studying related journals, attending seminars, inquiring of domestic and foreign organisations, Internet search queries, and formal and informal discussions with representatives from other organisations.</td></tr>
<tr><td>Process owner as a risk indicator</td><td>Process owners who have the knowledge and understanding to perform their jobs and can identify potential risks arising from the operation.</td></tr>
<tr><td>Internal information</td><td>Internal audit reports, consultation with the Risk Management Department, etc.</td></tr>
<tr><td>External information</td><td>Business articles, advice from external experts or regulators, etc.</td></tr>
</table>
</td></tr>
</table>

Process	Description	
	Analysis process map	Understanding current operations or good practice can help identify operational risks. Operational procedures may be in the form of process maps or descriptions, or both. The study of this data will help identify the risks of critical work procedures and internal controls that should be included.

Process	Description
2) Risk assessment	The risk assessment is a step that must be taken after risk identification. The process is to assess the likelihood and impact of the risk and the risk level in order to be prioritised. **I. Risk assessment** There are two levels of risk assessment: 1. **Inherent risk** is an existing risk of the organisation without any activity to reduce the likelihood and impact. 2. **Residual risk** is the remaining risk after the control activities are implemented, resulting in a change in the likelihood and/or impact. **Risk diagram before and after risk management**  Risk assessments will compare the severity of the risk and the risk appetite. If the level of risk is more than the risk appetite, the company needs to manage these risks promptly by formulating an additional risk management plan. The plan will help mitigate the risk so that it's within the risk appetite. **II. Criteria for measuring the severity of risk** The company will assess the severity of the risks to determine the risk response method and allocate resources to manage the risk appropriately. Risk assessments are considered in two dimensions: likelihood and impact. **Likelihood**: The likelihood of risk occurrences can be determined by the probability or frequency. **Impact**: The result of the damage caused to the company that affects the strategic plan and objectives can be considered in several ways in terms of both financial and non-financial values.

Process	Description

Likelihood criteria

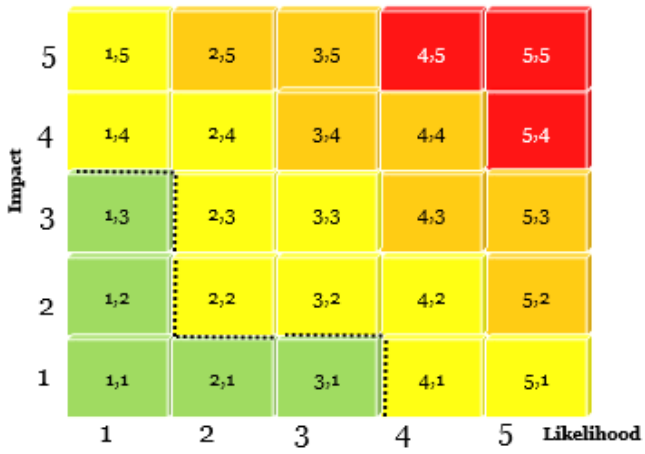
The level of risk likelihood and the impact of the damage caused by the risk can be divided into five levels and defined in each level as follows:

Rating	Rare (1)	Unlikely (2)	Possible (3)	Likely (4)	Almost certain (5)
Qualitative	Quite certain not to occurred.	Not likely to occur in normal situations.	Likely to occur in normal situations, there must be many driving factors.	Have occurred often, or has occurred every month.	Quite certain to occur, or high frequency of occurrence.
Frequency	Never occurred, or up to once in 3 or more years.	Once in 1 to 3 years.	Once in a year.	Once in 6 months up to 1 year.	Once every month.
Possibility	<10% chance of occurrence	10-40%	41-60%	61-90%	>90%

Impact criteria

The level of impact of the risk can be divided into these eight areas:

Impacts	Insignificant (1)	Minor (2)	Medium (3)	Major (4)	Critical (5)
Financial					
Financial loss	Up to 5MB	>5-10MB	>10-15MB	>15-20MB	>20MB
Impact on profit	Decrease <1%	1-2%	>2-5%	>5-10%	>10%
Cash flow impact	No impact	Can cover by operating	May be affected	Imminent cash flow problems	Has cash flow problems
Non – Financial					
Image & Reputation	Local media attention, no impact	Local media coverage in a few days	National negative media coverage 1-3 days	National negative media coverage >3 days	International negative media coverage, and social media
Law & Reputation	No report to regulator	Reportable incident to authorised parties, no follow up actions	Report to local governor with immediate actions	Report to regulator for corrective actions	Significant prosecution & fines
Safety & Environment	First aid treatment	Medical treatment injury	Single lost time injury	Multiple lost time injuries	Fatalities
Environment	Very low impacts	Low impacts	Moderate and internal impacts	Major impacts	Severe impact incidents, affect to external parties
Community	Isolated complaint	Sporadic or multiple complaints	Repeatable or serious of complaints	Ongoing complaints from concerned parties	High concern from various parties

Process	Description
	III. **Risk Map** After risk identification, the company will put the risk on the risk map in accordance with the potential risk and impact assessment by using the criteria for measuring the severity of the risks mentioned before.  The color space that appears in the risk map is consistent with the risk appetite of the company, and approaches to managing risk are varied according to the degree of risk.

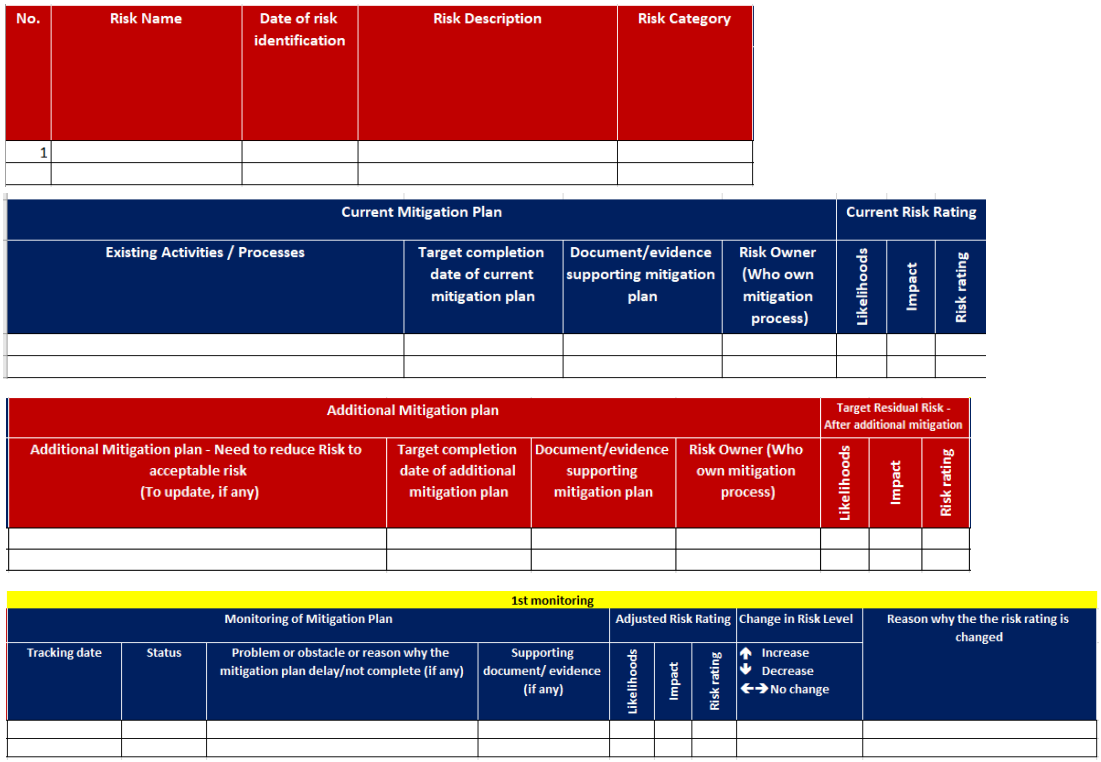
Risk level	Score	Status	Description
Low	1-3	Green	-Acceptable risk level without additional management or control
Moderate	4-9	Yellow	-Monitor the risk to prevent it goes to higher level '-Internal implementation report
High	10-16	Orange	-Unacceptable risk need to be decreased and monitored regularly '-Report to Chief Executive Officer
Critical	20-25	Red	-Must proceed immediately '-Report to Chief Executive Officer and Risk Management Committee

<table>
<tr><th>Process</th><th>Description</th></tr>
<tr><td>3) Risk management</td><td>
After risk assessment, if the severity of the risk is higher than the risk appetite level the management can choose to use risk-response methods based on the severity and priority of the risk, including the business environment and objectives.

Risk responses
<table>
<tr><th>Methods</th><th>Description</th></tr>
<tr><td>Accept</td><td>No action is taken to change the severity of the risk. This response is appropriate when the risk to strategy and business objectives is already within the risk appetite. Therefore, it is important for the company to ensure if the risk is within the risk appetite.

Risk that is outside the entity’s risk appetite and that management seeks to accept will generally require approval from the Board or other oversight bodies.</td></tr>
<tr><td>Avoid</td><td>Action is taken to remove the risk, which may mean ceasing a product line, declining to expand to a new geographical market, or selling a division. Choosing avoidance suggests that the organisation was not able to identify a response that would reduce the risk to an acceptable level of severity.</td></tr>
<tr><td>Pursue</td><td>Action is taken to accept the increased risk to achieve improved performance. This may involve adopting more aggressive growth strategies, expanding operations, or developing new products and services. When choosing to pursue risk, management must understand the nature and extent of any changes required to achieve the desired performance while not exceeding the boundaries of acceptable tolerance.</td></tr>
<tr><td>Reduce</td><td>Action is taken to reduce the severity of the risk. This involves any of myriad everyday business decisions that reduces risk likelihood, impact, or both.</td></tr>
<tr><td>Share</td><td>Action is taken to reduce the severity of the risk by transferring or otherwise sharing a portion of the risk. Common techniques include purchasing insurance products, engaging in hedging transactions, and outsourcing specialist service providers.</td></tr>
</table>

Steps to defining a risk management plan
1. To define risk management strategies, executives must consider the effectiveness of the risk management plan in terms of reducing the impact and/or the potential for risk to an acceptable level of severity.
2. Assign responsibilities and deadlines for implementation and the expected completion date (day, month, year) of the risk management plan by assigning risk owners to be responsible for specifying the details of risk management plans or required control activities, including the budget for implementation.
</td></tr>
</table>

Process	Description
	3. The risk owner is responsible for implementing the plan or monitoring the plan to ensure that the plan had been implemented properly and on time. **Example of Risk Assessment Template risk (including Risk Monitoring)**  **Techniques to define risk management plans** 1. Determine what the real cause of the risk is, and be aware that one risk may have more than one cause. 2. Define a risk management plan in accordance with the cause of risk. 3. Consider existing measures. A risk management plan shouldn't be a current activity. It should be an additional activity to reduce the risk to an acceptable level. 4. Consider if the risk management plan reduces the 'likelihood' or 'impact'. 5. Consider the suitability of the risk management plan, including the resources (people, money, and time) required to ensure that it is consistent with the risk level. 6. Create the risk management plan so that it's clear: 'How to do it'. 7. Identify the person who is responsible for the risk management plan. If there are many, it's necessary to identify a main responsible person who can perform and/or coordinate with other related persons, which leads to the achievement of the risk management plan. 8. Specify the expected completion date clearly (the day, month, and year). 9. If it's a continuous activity, specify the start time and frequency clearly (e.g. once a month or quarterly). 10. Monitor the effectiveness of the risk management plan to ensure that the risk is reduced.

2.2.3 Review and Revision

<table>
<tr><th>Process</th><th>Description</th></tr>
<tr><td>1) Assessing substantial change</td><td>After implementing the risk management framework, the organisation needs to regularly review and revise the framework to align with any substantial changes in the operational environment. This is to ensure the effectiveness of the control activity. Therefore, it is necessary for the executive to review the risk management frequently, since the factors associated with risk e.g. likelihood and impact might change. As might the cost of the risk management i.e. the resources utilised in the process of risk management.

Some examples of substantial change in business environment are highlighted below.

<table>
<tr><td rowspan="2">Internal environment</td><td>Rapid growth: When operations expand quickly, existing structures, business activities, information systems, or resources may be affected.

- Risk oversight roles and responsibilities may need to be redefined in light of organisational and geographical changes due to an acquisition.
- Information systems may not be able to effectively meet risk information requirements because of the increased volume of transactions.
- Resources may be strained to the point where existing risk response and actions break down.</td></tr>
<tr><td>Innovation: Whenever innovation is introduced, risk responses and management actions will probably need to be modified. For instance, introducing sales capabilities through mobile devices may require access controls specific to that technology. Training may be needed for users.</td></tr>
<tr><td rowspan="2">External environment</td><td>Changing regulations: Changes to regulations can result in changes in operating requirements. For example, changing the regulation on lending business.</td></tr>
<tr><td>Changing the economic environment: Changes in the economy can result in increased competitive pressures. For example, if new competitors provide new services such as lending through convenience stores.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Process</th><th>Description</th></tr>
<tr><td>2) Reviewing risk and performance</td><td>
Over time, an entity may not conduct its practices as efficiently as intended, thereby causing risk to arise and affect performance. From time to time, the organisation may wish to consider its enterprise risk management capabilities and practices.

Techniques to review and improve risk management

If an organisation determines that the performance doesn't fall within its acceptable variation, or that the target performance results in a different risk profile than what was expected, it may need to do the following:

<table>
<tr><td>Review business objectives</td><td>An organisation may choose to change or abandon a business objective if the performance of the entity is not achieved within an acceptable variation.</td></tr>
<tr><td>Review strategy</td><td>Should the performance of the entity result in a substantial deviation from the expected risk profile, the organisation may choose to revise its strategy. In this case, it may choose to reconsider an alternative strategy that was previously evaluated, or identify new strategies.</td></tr>
<tr><td>Revise risk appetite</td><td>Corrective actions are typically undertaken to maintain or restore the alignment of the risk profile with the entity's risk appetite, but can extend to revising it.</td></tr>
<tr><td>Revise risk responses</td><td>An organisation may consider altering or adding responses to bring risk in line with the target performance and risk profile.</td></tr>
</table>

The time and the person to review and improve the risk management

<table>
<tr><th>No.</th><th>Topic</th><th>Frequency</th><th>Responsible person</th></tr>
<tr><td>1</td><td>Review the risk management framework.</td><td>Annually</td><td>Board of Directors</td></tr>
<tr><td>2</td><td>Review risk appetite.</td><td>Annually</td><td>Board of Directors</td></tr>
<tr><td>3</td><td>Review the risk management manual.</td><td>Annually</td><td>Risk Management Department</td></tr>
</table>
</td></tr>
</table>

2.2.4 Information, Communication and Reporting

The organisation needs to set up an efficient information and communication system to support risk management and align with the defined risk management framework and processes. To achieve efficient risk management, necessary information from both internal and external sources, are required to be communicated in a proper, timely manner. Specifically, the information related to risk identification, assessment, and management should be shared throughout the organisation, thus encouraging the organisation to manage risk efficiently and effectively.

Process	Description
1) Communicating risk information	The company needs to encourage proactive communication to monitor issues such as changes in risk level, the progress of the risk management plan, and the effectiveness of risk management in the company. Continuing risk management is the best practice. However, management should set the risk monitoring as an agenda for discussion at meetings such as executive meetings, working group meetings, and Risk Management Committee meetings. Continuous communication can ensure that risk information is met and it can be used to make decisions swiftly. In some cases, informal channels may be more appropriate, for example, for urgent risks. A telephone discussion may be needed to decide and manage the risk immediately. **Examples of risk monitoring activities** 1. The risk owner monitors the implementation of the risk management measures regularly. This may be done by recording and evaluating the performance of risk management activities. It may be evaluated by the duration or progress of the activity. 2. The Risk Management Department coordinates with risk owners to monitor the implementation of the risk management measures at least every quarter. 3. The management monitors and supervises risk management activities through regular meetings or ad hoc meetings. 4. Meetings of the working group to follow-up on specific issues. 5. Performance measurement based on performance indicators include, for example, key performance indicators (KPIs), scorecards, or milestones. 6. Consideration and analysis of serious incident reports or unexpected events. 7. Performance benchmarking. 8. Survey of co-operators or persons affected by risk management. 9. The results of an internal audit that reviews the compliance of a policy, process or procedure established to manage the risk. **Monitoring the progress of the risk management plan** Risk monitoring based on the progress of the risk management plan is regarded as a simple format. The owner of the risk is responsible for monitoring the risk management plan implementation to ensure it's in line with the plan and time frame. Then, it's required to record the status of the track that has already been processed, pending, delayed, or has not started. The main objectives of monitoring the progress of the risk management plan include: - To ensure the risk management plan is implemented. - To evaluate the efficiency and effectiveness of the risk management plan that helps reduce the risk level.

Process	Description
	- To assess the adequacy of the defined risk management plan. If the risk management plan can't reduce the risk level, the executives need to consider establishing additional risk management plans or revising the risk management plan. - To consider changes in the operation, new potential risks, or changes in the risk due to changing operational environment. Risk and control activities are constantly changing. Risk management plans or control activities may be less effective due to non-compliance with the plan. This also includes changes in the objectives or processes. Therefore, the management must regularly assess risk management to ensure that risk management remains effective in accordance with the risk monitoring form.

<table>
<tr><th>Process</th><th>Description</th></tr>
<tr><td>2) Risk reporting</td><td>

Principles of risk reporting

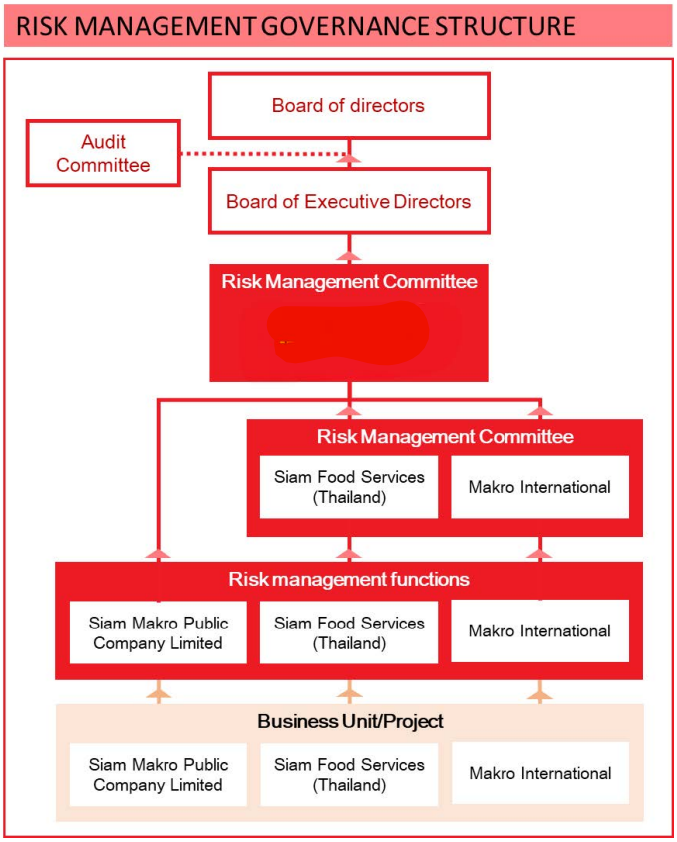
The significant risks must be reported to the Board of Directors, Executive Committee, and the Risk Management Committee. The report must be concise, accurate, and prompt, which brings about an efficient and effective risk management follow-up. Basically, the reporting will focus on key risks and activities to mitigate the risk. After the risk management framework has been implemented for a certain period, the company may adjust the format or the reporting frequency, such as reporting the key risk and the risk status every quarter. The risk reporting regarding risk management will help:

- the Board of Directors to ensure that the risk is within risk appetite
- the Heads of departments and senior executives to identify and understand risks at both the strategic and operational levels and assess the effectiveness of current risk responses, and
- the heads of departments and senior executives to ensure that critical risk control is effective or additional measures should be taken.

Reporting frequency

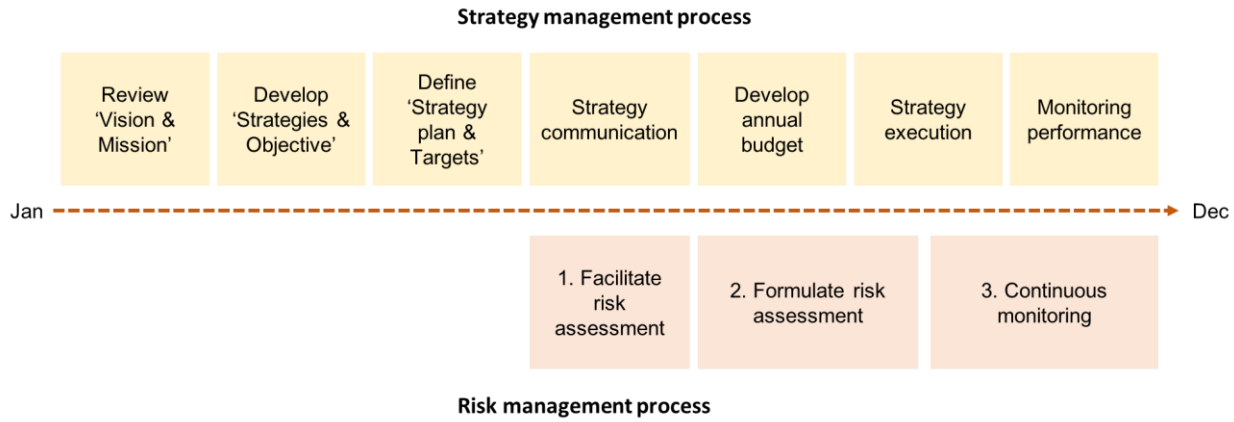
<table>
<tr><th>No.</th><th>Report</th><th>Responsible person</th><th>Frequency</th></tr>
<tr><td>1.</td><td>Corporate risk</td><td>Risk Management Committee</td><td>At least every quarter</td></tr>
<tr><td>2.</td><td>Risk register</td><td rowspan="2">Risk Management Department / Working group</td><td>At least every quarter</td></tr>
<tr><td>3.</td><td>Risk map</td><td>At least every quarter</td></tr>
<tr><td>4.</td><td>Progress report on the risk management plan</td><td>Risk owner</td><td>At least every quarter</td></tr>
<tr><td>5.</td><td>Risk indicator report</td><td>Risk owner</td><td>At least every quarter</td></tr>
</table>

</td></tr>
</table>

Process	Description
	Risk reporting map The Risk Management Department will develop a risk profile and risk map, follow up on progress reports on the risk management plans, and present them to the Risk Management Committee. The Risk Management Committee of Siam Food Services (Thailand) and Makro International will make a report for the Risk Management Committee. Next, the Risk Management Committee will report the major risk, activities, and result of the risk management to the Board of Directors and the Board of Executive Directors.  **Note** In the risk management meeting, the Risk Management Department may consider inviting the risk owner to attend the meeting to clarify and present risk and risk management plans.

Application of risk management for business

Enterprise risk management is integral to achieving strategy and business objectives. Well-designed enterprise risk management practices provide management and the board of directors with a reasonable expectation that they can achieve the overall strategy and business objectives of the company.



1. Facilitate risk assessment formulation (October – December)

1.1 Corporate risk assessment

- **Risk management department shall formulate corporate risks by analysing information** from:

  Internal information:

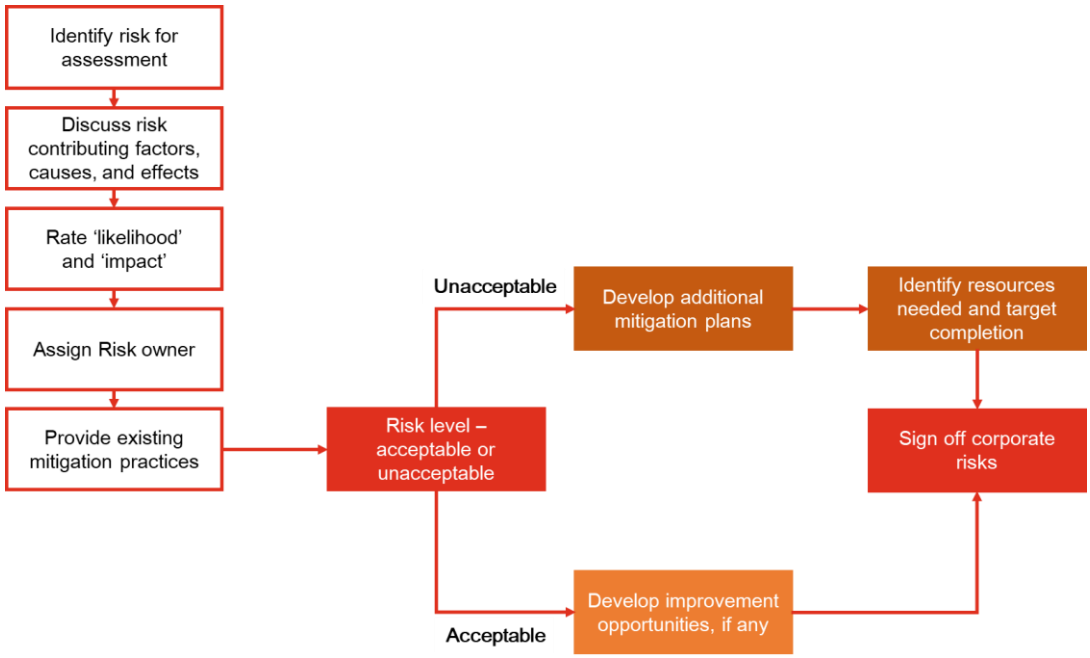
  - Strategic plan, business objectives and goals
  - Losses or incidents
  - Preexisting risk assessments and mitigation plans
  - Internal audit risk assessments and reports
  - Budget models and underlying assumptions/sensitivities as well as histories of reforecasts
  - Financial reports
  - Insurance coverage details and claims history
  - History of litigation and contracting
  - KRIs and KPIs
  - Interviews – a series of interviews should be conducted with management to:
    - Enable to refresh risk areas for inclusion in the draft risk profile
    - Raise awareness amongst participants of the benefits/process of risk profiling

External information: industry risk information (available through industry reports or publications)

- Media articles on the organisation
- Analyst reports on the organisation and its competitors
- Ratings agency reports on the organisation and its competitors
- Reports on industry outlook prepared by analysts

- **Risk management department shall undertake a brainstorming session or a survey to develop this preliminary list of risks** prior to involving a broader range of staff and management based on the information that has been gathered, develop, discuss, and agree upon a draft risk profile. The profile should comprise a high-level indication of relevant corporate risks, supported by specific contributing factors. Then, Risk management department shall send the draft corporate risk assessment to the workshop participants for review prior to the actual risk assessment workshop.

- **Risk management department shall arrange with management and conduct the corporate risk workshop** to discuss the events/risks may face for the upcoming year. The corporate risk workshop process is illustrated in the diagram below:



- **After the corporate risk assessment workshop, Risk management department shall communicate the assigned risk owners to pursue further analyse the risks.** With the facilitation of the Risk management department, risk owner shall develop risk assessment, determine the targeted completion date, and establish KRIs (if needed).

1.2 Business risk assessment:

- **Head of the departments shall communicate the related approve strategies, objectives, and goals within departments.**

  It is important to begin by understanding the relevant business objectives in scope for the risk assessment. These will provide a basis for subsequently identifying potential risks that could affect the achievement of objectives, and ensure the resulting risk assessment and mitigation plan is in alignment with the strategies, objectives, and goals of the company.

- **Risk champion shall develop the risk assessment based on related strategies, objectives, and goals of the company.**

  Risk champion shall use the risk assessment template provided by Risk Management department based on risk management framework decribed in this manual. Risk champion can choose to discuss and identify the risks that could impair the success of each core strategy and complete the risk assessment within own department, or request for a support from Risk management department team. Risk management department shall support the department, upon request, by phone call, email, facilitating the risk assessment session (within department) or a workshop (cross departments, if needed) to demonstrate the risk assessment and ensure all risk details are captured. Risk Champion shall complete the risk assessment by providing informations in all topics provided in the template.
  Risk Committee or Management may identify the risk for the department which Risk management department shall communicate such risks to Risk champion promptly to include in the assessment.

- **Risk champion shall develop and update the Key Risk Indicators (KRI).**

  Not all risks must have KRI, shall develop KRI for the organization’s top risk exposures. Risk department team shall work in concert with the risk owners to identify appropriate key risk indicators, trigger points and mitigation plans to be initiated in the event those points are reached. Risk champion shall update KRI data and submit to Risk management department. Risk Committee may only require updates of the most significant KRI data in order to be confident that the risk management process is functioning as designed and approved.

- **Risk champion shall propose the risk assessment to the head of the department for validation and endorsement.**

  The risk assessment must be agreed by the head of the department before submitting to Risk management department. If the risks identified is considered a key risk which may impact the company at the organizational level, the head of department, Risk owner, shall be required to present such risk to Risk Committee. Risk management department shall make an appointment in advance and support Risk owner and Risk champion for the preparation.

2. Formulate risk assessment (Mar, Jun, Sep, Dec)

- **Risk management department shall review and develop consolidated the risk assessment.**

  Risk management department shall perform the following:
  - Determine whether risk profiles cover all major risk classes and risks were appropriately categorised.
  - Check that risk descriptions provide sufficient information, including: Key causes (why the risk might arise), Key impacts (what impacts the risk could have) and the trend of the risk – is it decreasing, stable, or increasing, and Assumptions underlying the impact assessments made (if relevant).
  - Check that current controls or mitigations have been captured during the risk assessment and their effectiveness determined. This will help to determine the current organisation vulnerability to a risk and should be documented in the outputs from the risk assessment process, for example in the risk register
  - Check that further risk mitigation actions are documented, including ownership, accountabilities, and time frames
  - Check that important monitoring and measurement mechanisms have been considered and documented
  - Check whether risk identification and assessment activities are performed regularly and kept up to date

- **Risk management department shall perform a high-level check** of the level of accuracy and representation is required (how well the existing risk profile actually represents the risks faced by the company). To do this an important step, consider the following:
  - Separate the significant risks from the rest of the risk assessment or the risk map
  - Discuss the top risks with the management and Risk Committee to validate their significance
  - Check the top risks with the disclosed risk information of similar organisations; check globally if no information is disclosed for the local organisations

- **Risk management department shall ensure that an appropriate cross-section of management from across the organisation are consulted** with and provided with an opportunity to contribute their accumulated knowledge and experience to the risk assessment. Risk management department may set up a session with management who possesses knowledges or is considered an experts within area such as human resources, operations, legal for a session to provide views on specific risk. This is to yield valuable information based on the unique knowledge of staff and management and help raise awareness about risk management within the organisation.

- **Risk management department shall ensure the quality of the risk assessment** and may request for further supporting information from risk owners.

3. Continuous monitoring (Jan-Dec)

- **Risk champion shall update the risk assessment quarterly**, this includes reviewing the status of the mitigation plan, provide additional mitigation plans, if any. Risk management department shall notify Risk champion 3 weeks in advance of the quarterly Risk Committee meeting.
- **Risk champion shall update the KRI status to Risk management department** Risk management department shall review, consolidate, and report Corporate risks to management and RC, respectively. This will help trigger the warning so that the necessary decisions/actions can be made in time.
- **Risk management department and Risk champion shall routinely monitor emerging risks** by regularly performing a thorough scan of characteristics and changes in the environment to identify events that may have impacted the organisation’s shareholder value in the past or may impact it in the future. Drivers to consider include economic, social, political, technological, and natural environmental events, all of which can be identified through external sources such as media articles, analyst and rating agency reports, and publications by not-for-profit foundations. The emerging risks shall be report to Risk Committee for consideration, if they were to impact the company. Such risk will be assessed, assigned risk owner, and communicated to related functions.

Part 3 Appendices

3.1 Glossary of key terms

Terms		Description
Business unit / Departmental risk	ความเสี่ยงระดับหน่วยงาน	The risk that may arise from the operation of each department, unit and project. The risk can be managed by the department, unit and project or controlled by the existing internal control activity.
Control activity	กิจกรรมการควบคุม	The policies, procedures, techniques, and mechanisms that help ensure that management's response to reduce risks identified during the risk assessment process is carried out.
COSO	The Committee of Sponsoring Organisation of the Treadway Commission	COSO is a joint initiative of the five private sector organisations listed below and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control and fraud deterrence. 6. American Accounting Association 7. American Institution of Certified Public Accountants 8. Financial Executives International 9. Institute of Management Accountants 10. The Institute of Internal Auditors
Corrective controls	การควบคุมเชิงแก้ไข	A design to correct errors or risks, or mitigate the impact from negative events and errors.
Detective controls	การควบคุมเชิงค้นหา	A control mechanism that finds problems in a company's processes to enable proper corrective measures.
Enterprise Risk Management	การบริหารความเสี่ยงขององค์กร	The culture, capabilities, and practices integrated with strategy-setting and its performance, which organisations rely on to manage risk that might affect the corporate value.

Terms		Description
Impact	ผลกระทบ	The result or effect of a risk that might cause a range of possible types of impact. The impact of a risk may be positive or negative relative to the entity's strategy or business objectives, including: - Financial impact - Reputational impact - Regulation and compliance impact
Inherent risk	ความเสี่ยงที่มีอยู่	An existing risk of the organisation without any activity to reduce the likelihood and impact.
Internal control	การควบคุมภายใน	A process, put into effect by an entity's Board of Directors, management, and other personnel, which is designed to provide reasonable assurance regarding the achievement of objectives relating to the following: • Effectiveness and efficiency of the operation • Reliability of the financial report • Compliance with related laws and regulations
Likelihood	โอกาสเกิด	The possibility that a risk will occur based on the probability of occurrences or the frequency of events.
Monitoring	การติดตามผล	The process of regularly reviewing, observing, and recording the progress, the control activity or system to locate changes.
Preventive controls	การควบคุมเชิงป้องกัน	Preventive controls are used to keep a loss or an error from occurring.
Reasonable assurance	การให้ความเชื่อมั่นอย่างสมเหตุสมผล	Acknowledgment that regardless of the good design of the risk management system, the achievement of the organisation's goals can't be guaranteed due to the limitations of the risk management of the organisation.
Residual risk	ความเสี่ยงที่เหลืออยู่	The amount of risk or danger associated with an action or event remaining after natural or inherent risks have been reduced by risk controls in order to improve the likelihood and impacts of the risk.

Terms		Description
Risk	ความเสี่ยง	The possibility that events will occur and affect the achievement of strategy and business objectives.
Risk appetite	ระดับความเสี่ยงที่องค์กรยอมรับได้	The types and amount of risk, on a broad level, an organisation is willing to accept in pursuit of value.
Risk assessment	การประเมินความเสี่ยง	The identification, evaluation, and estimation of the levels of risks involved in a situation to prioritise risks.
Risk factor	ปัจจัยเสี่ยง	The root cause which can determine the proper risk response measure. Risk factors are determined by internal and external factors such as corporate regulations, work processes, the economy, society, politics, customers, competitors, etc.
Risk identification	การบ่งชี้/ระบุความเสี่ยง	The process of determining risks that could potentially prevent the organisation from achieving its objectives by considering what, why, and how.
Risk map	แผนภาพความเสี่ยง	A data visualisation tool for communicating specific risks an organisation faces, showing likelihood and the impact of an occurrence.
Risk owner	เจ้าของความเสี่ยง	A person who is ultimately accountable for ensuring the risk is managed to achieve the objectives according to the time frame, responsible for monitoring their risks and executing risk responses when appropriate, and reports the events to the Risk Management and Risk Management Committee. Also, risk owners are the ones who are significantly affected by the risk, or are directly associated with the risk.
Risk Register	ทะเบียนความเสี่ยง	A tool for documenting risks, and actions to manage each risk, and to fulfill regulatory compliance acting as a repository for all risks identified, which includes additional information about each risk, e.g. objectives, nature of the risk, reference and owner, current mitigation measures, risk management plans, responsible persons, and deadlines.

Terms		Description
Risk Response	การตอบสนองความเสี่ยงการจัดการ/ความเสี่ยง	Risk response is classified into the following categories: (1) Accept (2) Avoid (3) Pursue (4) Reduce (5) Share
Stakeholders	ผู้มีส่วนได้เสีย	Parties that are affected by the organisation's operations e.g. shareholders, community, employees, customers, and salespeople.

Sources: (1) http://www.coso.org

(2) กรอบโครงสร้างการบริหารความเสี่ยงขององค์กรเชิงบูรณาการ : บทสรุปสำหรับผู้บริหารและกรอบโครงสร้าง, กรุงเทพฯ : ตลาดหลักทรัพย์แห่งประเทศไทย, 2551

(3) COSO (Enterprise Risk Management – Integrating with Strategy and Performance, June 2017)