Central Plaza Hotel Public Company Limited

Risk Management Framework

(2026 Edition)

Approved by Board of Directors Meeting NO. 7/2025

On 14 November 2025

Prepared by Risk Management Department

PUBLIC

Risk Management Framework (Edition 2026)

Central Plaza Hotel Public Company Limited

The main objective of the company's business operations is to create value for all stakeholders, including shareholders, customers, partners, employees, the government, and the general public. However, in conducting its business, the company faces risks that may either increase or decrease its value, making effective risk management essential. However, the company manages risks systematically in accordance with international standards (COSO Enterprise Risk Management Framework: COSO ERM) and integrates risk management with strategic planning and business operations to create, preserve, and realizing value for the organization. This is carried out by the Board of Directors, executives, and other personnel to support strategy formulation and operations across the entire organization. The risk management framework is designed to identify potential events that could impact the organization and to manage risks to an acceptable level, thereby providing reasonable assurance in achieving the organization's objectives.

1. Definition

- **Risk** is the possibility that events will occur and affect the achievement of strategy and business objectives.
- **Enterprise Risk Management** is the culture, capabilities, and practices, integrated with strategy-setting and its performance, that organizations rely on to manage risk in creating, preserving, and realizing value.
- **Risk Appetite** is the size, amount, or level of risk that the organization can accept to create value while still enabling the organization to achieve its goals may be a single value or a range, depending on the appropriateness of each factor, and must be approved by the board of directors. This is used for risk assessment and management. If any risk, upon analysis and evaluation, is found to potentially impact the company beyond the acceptable risk level, the responsible department must prepare a risk management plan (Action Plan) and report it to the Risk Management, Corporate Governance and Sustainability Committee for consideration and presentation to the board of directors.
- **Risk Inventory** is all risks that could impact an entity
- **Risk Profile** is a composite view of the risk assumed at a particular level of the entity, or aspect of the business that positions management to consider the types, severity, and

interdependencies of risks, and how they may affect performance relative to the strategy and business objectives.

- **Risk Factors** are the origin or cause of a risk and the events that may prevent the achievement of the set objectives or goals. The identified cause of the risk should be the actual cause that can explain how this risk factor leads to specific risks and should be manageable with appropriate measures to mitigate the risk accurately.
- **Risk Assessment** is the process of identifying the severity level and prioritizing the significance of risk factors. This is achieved by evaluating the likelihood of occurrence (Likelihood) and the potential impact (Impact) that may arise.

2. Roles and Responsibilities in Risk Management

- **Board of Directors**

  The Board of Directors is responsible for determining corporate policies and strategic directions, as well as overseeing that the company has in place an efficient and effective risk management system to ensure risk management is prioritized and instilled as part of corporate culture.

- **Risk Management Corporate Governance and Sustainability Committee**

  Risk Management Corporate Governance and Sustainability Committee is responsible for determining risk management direction, approving risk management framework to be used as a guideline of practice, monitoring risk management results, raising awareness and understanding about risk management among employees across every level, ensuring risk management implementation throughout the organization, providing opinions/suggestions, giving advice to the management, and reporting to the Board of Directors.

- **Chief Executive Officer and Executives**

  Chief executive officer and the management are responsible for establishing risk management system in compliance with the policies and guidelines of the Board of Directors, considering and determining risk management strategies, overseeing the preparation of and monitoring risk management plans throughout the organization, defining and assigning risk owner responsibilities, considering and determining risk appetite to be presented to the Board of Directors for approval, communicating and developing risk culture, and reviewing the appropriateness of risk management system and measures.

- **Risk Owner**

  Risk owner is responsible for assessing and analyzing risks, formulating risk management measures/activities, analyzing cost-benefit of each option, monitoring risk assessment results, and presenting those results to Chief Executive Officer and Risk Management Corporate Governance and Sustainability Committee.

- **Risk Management Department**

  Risk management department is responsible for developing an effective and efficient risk management system, giving advice and recommendations, organizing trainings to ensure proper understanding of risk management and ultimately instilling risk culture within the organization, coordinating with and monitoring risk assessment results prepared by risk owner and relevant persons for creating risk assessment report to be presented to the management and Risk Management Corporate Governance and Sustainability Committee and/or the Board of Directors.

- **All Employees**

  Employees are responsible for complying with the risk management policy and process of the company, including complying with other guidelines or orders issued by the Board of Directors or Risk Management Corporate Governance and Sustainability Committee.

3. Risk Management Framework

The company has established a risk management framework based on the international standard (COSO Enterprise Risk Management Framework: COSO ERM), which integrates enterprise risk management with strategy and performance. This approach clarifies the importance of enterprise risk management in strategic planning and its significance in being applied across the entire organization. The framework is divided into five interrelated components as follows:

1) Governance & Culture

The company has structured and clearly defined responsibilities for risk management, including fostering a corporate culture that emphasizes awareness of risks that may impact business operations.

2) Strategy & Objective-Setting

The company has a strategic planning process that integrates risk management principles and develops strategies and business objectives that align with acceptable risk levels.

3) Performance

The company identifies and assesses risks that may impact the success of its strategies and business objectives. These risks are prioritized based on their level of impact and the likelihood of events that may cause them. Additionally, the company establishes appropriate risk response methods. The outcomes of this process are reported to key stakeholders involved in the risk.

4) Review & Revision

The company regularly reviews its performance to evaluate the effectiveness of its risk management. It also reviews its risk management practices to ensure continuous improvement.

5) Information, Communication & Reporting

The company has an information system that promotes effective risk management. This system supports risk data, performance data, and the preparation of risk management reports to ensure continuous and appropriate communication of risk management results to stakeholders.

4. Risk Management Process

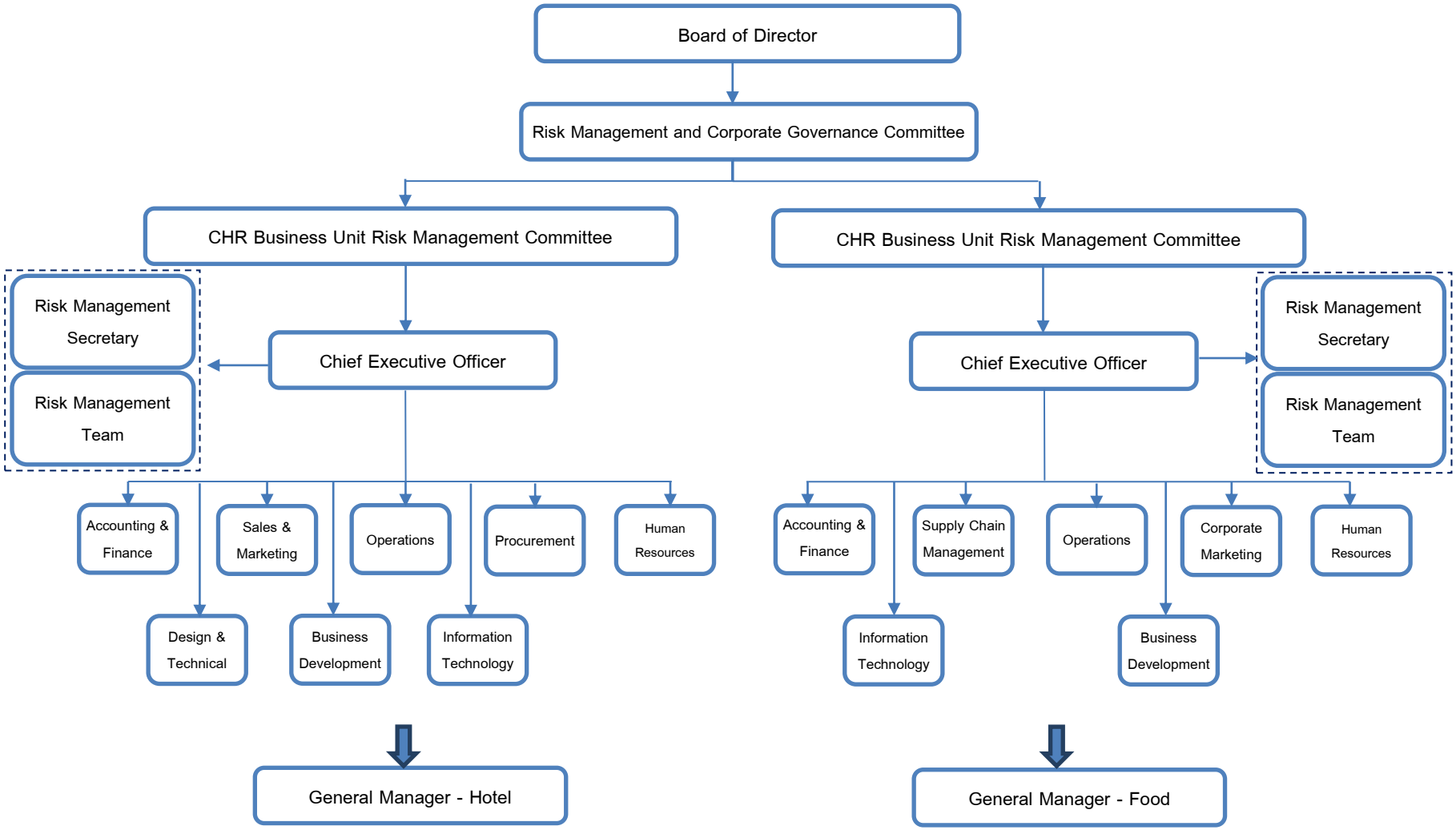
The organization's risk management is a continuous process that encompasses all levels of operations, including departments, divisions, business units, operational activities, and various projects. This ensures that risk management is integrated into every level of the organization's operations.

The risk management process involves the participation of personnel throughout the organization in thinking, analyzing, and forecasting potential events or risks. It also includes identifying ways to manage these risks to an appropriate or acceptable level. This process helps the organization achieve its desired objectives in line with its vision and mission framework.

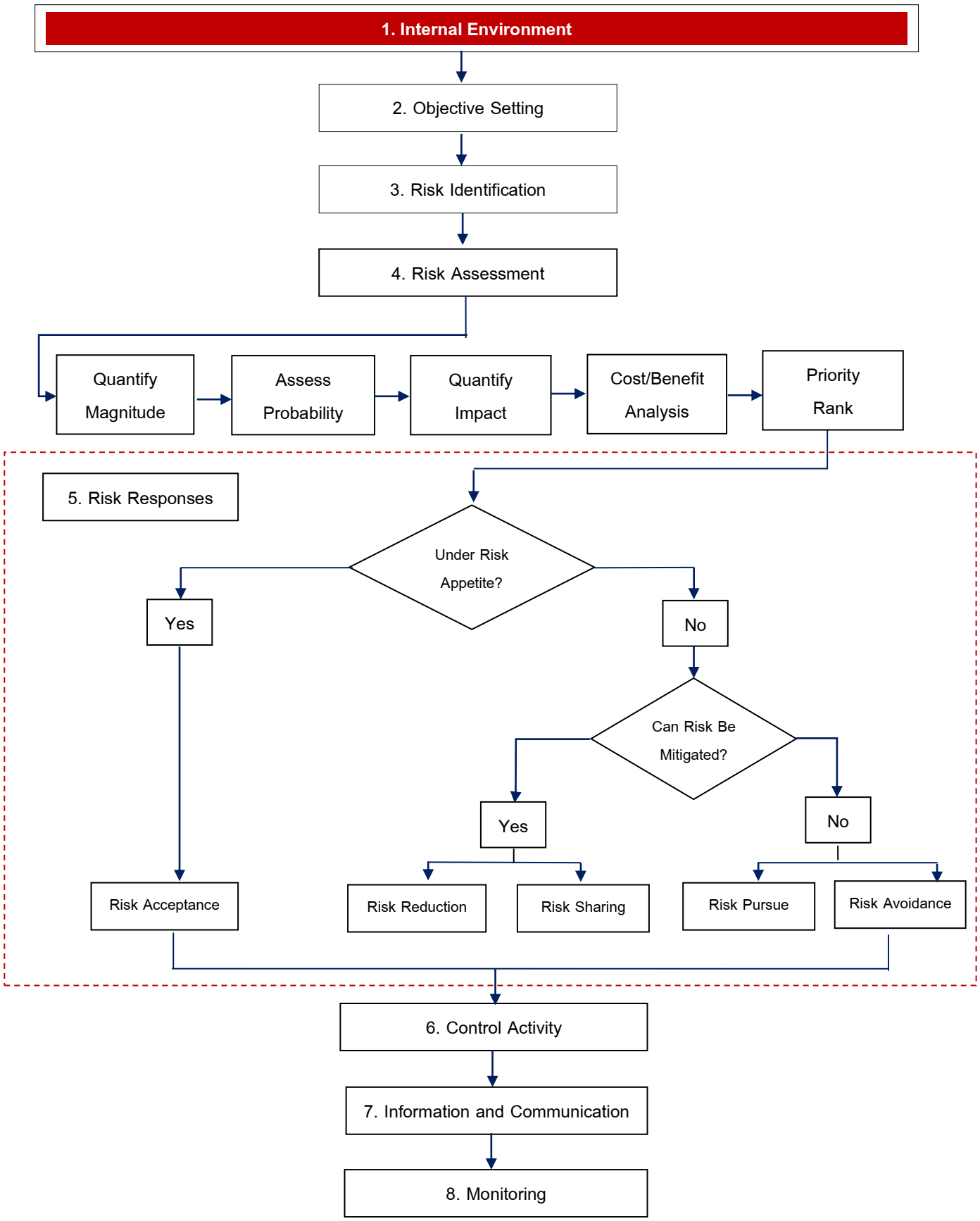
The company has established a risk management process to ensure that the steps and methods for managing risks are systematic and aligned throughout the organization. This consists of 8 steps as follows:

1) Internal Environment
2) Objective Setting
3) Risk Identification
4) Risk Assessment
5) Risk Responses
6) Control Activities
7) Information and Communication
8) Monitoring

Risk Management Structure of Central Plaza Hotel Public Company Limited



Risk Management Process Flowchart



The key steps of the organizational risk management process consist of 8 steps as follows.

4.1 Internal Environment

The internal environment of the organization is a crucial factor in determining the direction of the organization's risk management framework. This includes several factors, such as organizational culture, management policies, employee practices, work processes, information systems, and so on.

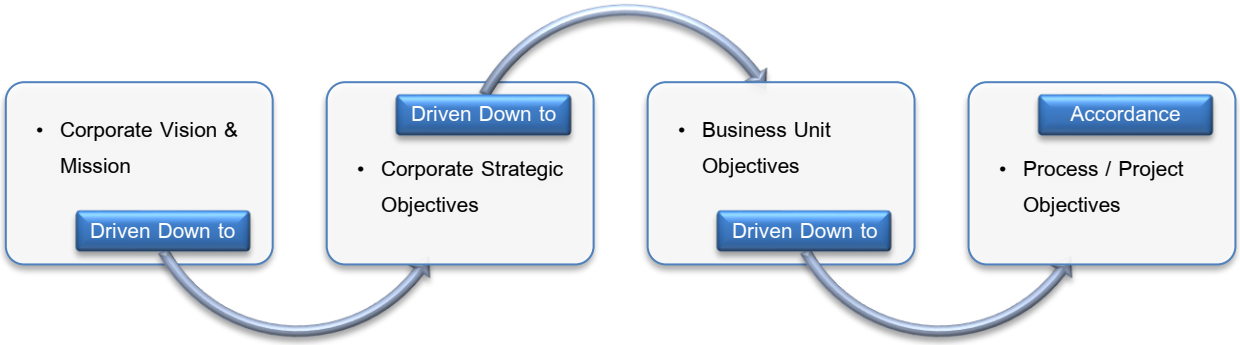
Organizational culture develops through the participation of employees at all levels. Since each member and employee of the organization has a different understanding of risk management, there are varying methods for identifying, assessing, and responding to risks. Having a consistent organizational culture helps ensure that employees understand risk management in a unified way.

4.2 Objective Setting

Setting objectives within the organization must be consistent and aligned to ensure that the activities carried out by departments, management, and employees support the achievement of the organization's objectives.

Setting objectives for risk management must be aligned with the organization's strategy and risk appetite, in order to establish clear and appropriate risk management goals for the organization.

The image below illustrates the alignment of objectives at different levels that the company should have.



Objective Setting Process

1. The company's board of directors and top-level executives establish the company's vision, mission, and strategic objectives. Following that, they set overarching goals that align with and support the achievement of the company's vision and mission.
2. The company's board of directors and top-level executives assess the types and levels of risk that the company is willing to accept (Risk Appetite) and establish business strategies that align with the acceptable level of risk for the company. This is used as a guideline for formulating coherent business strategies.
3. Executives define objectives at the operational, process, or project levels that are significant and aligned with the company's business strategy. The set objectives should have a clear relationship with the company's strategic goals and contribute to achieving them. Even though different objectives may have varying levels of importance, setting objectives should follow the 'SMART' principles to the greatest extent possible.

Setting SMART Objectives

Objectives must be clear and aligned with the principles known as SMART, as follows:

Subject	Description
Specific	Objectives should be clear, specific, and avoid ambiguity to ensure mutual understanding.
Measurable	Objectives should be measurable in both quantitative and qualitative aspects and should include specified criteria and the required data for measuring outcomes.
Achievable	Objectives should be realistic, reasonable, achievable, and feasible given the available resources and constraints, such as market conditions, timeframes, resource allocation, and more.
Relevant	The returns or outcomes of the defined objectives must align with and support the achievement of higher-level objectives.
Time bound	Objectives should have a clearly defined timeframe for achievement.

4.3 Risk Identification

Risk Identification involves gathering events that may pose risks to the organization's objectives. Management must consider all potential risks that could arise. This process might include interviewing senior executives or managers responsible for specific plans or operations and addressing key risk issues of concern. The outcome is a Corporate Risk Profile, which outlines significant types of risks that could prevent the organization from achieving its vision, objectives, or goals. These risks may either have the potential to occur in the future or be events that could lead to lost business opportunities. Risk identification should be considered both internal and external factors.

1) Internal factors are risks from things we can control, set, or from our own capabilities. These include the organization's objectives, policies and strategies, operations, work processes, organizational structure, organizational culture, as well as the organization's capabilities in terms of resources and knowledge, such as funding, time, personnel, processes, systems, and technology.

2) External factors are risks that we cannot control, arising from external influences that we need to find ways to manage. Examples include government policies, economic/social/political conditions, competition, wars, and natural disasters.

Type of Risks

The company has categorized types of risks as follows:

- **Strategic Risk**

  This is a risk arising from the establishment of inappropriate strategic plans or management policies, or those not aligned with various factors such as government policies, legal changes, public issues, failure to meet revenue targets, unclear investment plans, etc., which prevents the organization from achieving its objectives or goals.

- **Financial Risk**

  This is a risk arising from a lack of data, analysis, planning, control, and reporting used for proper financial management, affecting the organization's financial status or stability. It also relates to financial liquidity issues, such as interest rate fluctuations, exchange rate fluctuations, and risks arising from counterparty issues, among others.

- **Operational Risk**

  This is a risk that every business inevitably faces, arising from personnel, work processes, technology, and external factors. This risk occurs from the normal operations of a business, but the business must find ways to control and manage

these risks to prevent them from happening. If a business allows operational risks to accumulate, the business's performance may not meet expectations and could have damaging effects, such as delays, lack of effective equipment, or IT system failures.

- **Compliance Risk**

  This is a risk arising from violations or non-compliance with laws, regulations, rules, or standards related to operations. Existing laws may pose obstacles to operations, and the policies and procedures established by the organization may be unfeasible. For example, this risk includes failing to fully comply with new laws or confusion in selecting which rules/regulations to enforce.

  - **Corruption Risk**

    This is a risk arising from any actions taken to seek unlawful benefits, such as offering or receiving bribes, whether in the form of money, goods, political assistance, charitable donations, hospitality expenses, or other costs. This includes proposing, promising, or committing to give, demanding, offering, or receiving money or any other inappropriate benefits to government officials, government agencies, private entities, or individuals, either directly or indirectly, in order to influence them to perform or refrain from performing their duties improperly.

- **Cyber Risk**

  This is a risk related to cybersecurity issues arising from changes in information technology, including digital transformation. This affects the company's operations and encompasses the information technology systems that the organization uses for critical business activities.

- **Climate Change Risk**

  This is a risk related to changes in climate conditions and related impacts, which may affect business operations, supply chains, and the organization’s overall sustainability.

4.4 Risk Assessment

Risk assessment is a process that includes analyzing, evaluating, and ranking risks that impact the achievement of an organization's or unit's objectives. It should assess whether these risks have a positive or negative impact on achieving the objectives. Risk assessment involves comparing the level of risk obtained from risk analysis with the acceptable risk level (Risk Appetite). If the risk level is not within the acceptable threshold, the risk will be managed promptly.

This involves considering both inherent risk (the risk before controls), residual risk (the risk after controls), and target risk (the desired risk level).

1) Inherent Risk

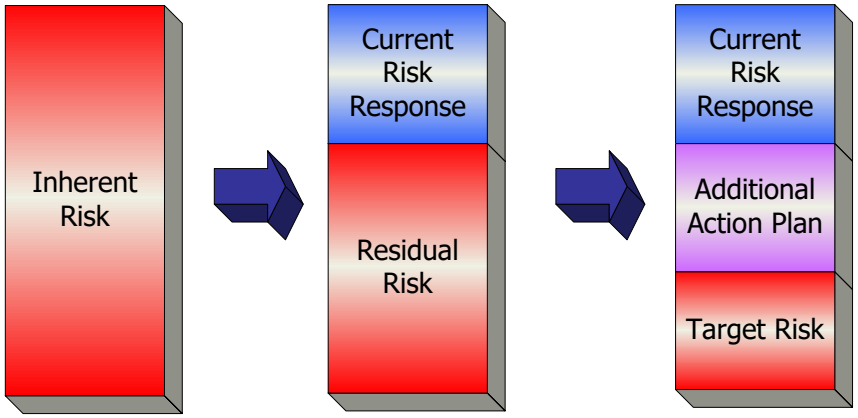
Inherent risk is the risk faced by an organization before any actions have been taken by management to reduce its impact or likelihood. Assessing inherent risk allows management to estimate the resources needed and the level of control required to manage the risk.

2) Residual Risk

Residual risk is the risk that remains after implementing current activities to manage the risk. Assessing residual risk allows management to determine whether the existing controls are effective enough, insufficient, or excessive. After evaluating residual risk, if management wishes to further reduce the risk level, they can develop additional risk management plans.

3) Target Risk

Target risk is the level of risk that the organization aims to achieve after implementing the risk management plan.



This diagram illustrates the sequence for assessing risk, where management can follow these steps:

- Evaluate inherent risk.
- Apply current risk responses to assess residual risk.
- Define the target risk level by creating additional risk management plans to reduce the risk to the desired level.

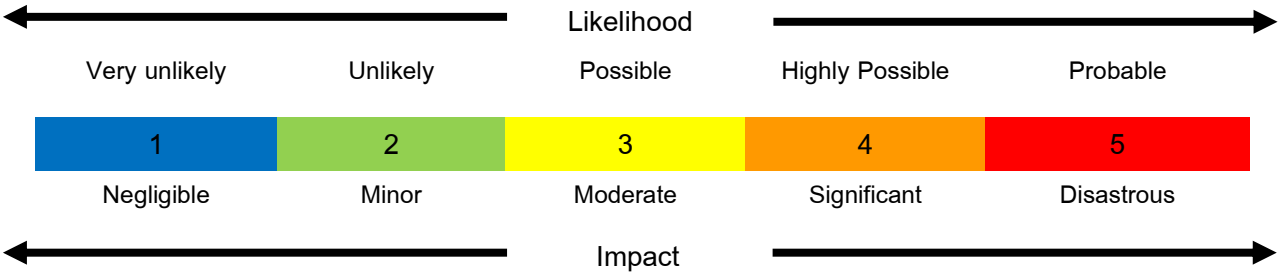
Setting Risk Criteria

The criteria used for assessing risks should reflect the value, objectives, and resources of the organization. Some criteria may be developed from legal requirements or regulations set by regulatory bodies or member organizations. The established criteria must align with the organization's risk management policies and be reviewed continuously.

Risk assessment considers the likelihood of risks occurring and the impact of risk events to prioritize their significance. A risk map is used to classify and visualize risks, define acceptable risk levels, and establish key risk indicators (KRIs).

- **Likelihood** refers to the probability of a risk event occurring within a certain period, which can also be described as the frequency or chance of the risk event happening.
- **Impact** refers to the severity of the damage or consequences that the risk may cause, which affects the organization both positively and negatively. Impacts can be categorized into financial impacts and non-financial impacts.

Management can assess the level of likelihood and impact of risks by assigning scores ranging from 1 to 5. The diagram below illustrates the approach for evaluating likelihood and impact.



The risk assessment criteria must be approved by the Risk Management Corporate Governance and Sustainability Committee and should be reviewed regularly to ensure alignment with changes in the business environment

➢ **Likelihood Assessment Criteria**

The criteria for assessing the likelihood of risk are established to evaluate the level of probability or chance that a risk event will actually occur. This assessment should consider both internal and external factors affecting the risk environment. The criteria are defined in 5 levels as follows:

Criteria	Very unlikely	Unlikely	Possible	Highly Possible	Probable
Likelihood	(1)	(2)	(3)	(4)	(5)
L:1 Amount of chance	Chance < 10% or Or 1 time a year	Chance 10–25% or 2 times a year	Chance 26–50% or 3-4 times a year	Chance 51–75% or 5-12 times a year	Chance > 75% or >12 times a year
L:2 History of Incidents	Never occurred before in the hotel/food industry.	Occurred before in the hotel/food industry but never in the company.	Occurred 1-3 times in the company.	Occurred frequently in the company 3-5 times.	Occurred very frequently in the company, more than 5 times.
L:3 The state of the actual situation	The real cause of the incident has been resolved and preventive measures have been taken to reduce the likelihood of recurrence.	The real cause of the incident is currently being resolved and establish preventive measures.	The incident can be resolved/closely monitored.	The incident is being resolved.	The incident was reported and is currently under investigation by both internal and external regulator.

➢ **Impact Assessment Criteria**

The criteria for assessing risk impact are established to evaluate the level of damage or severity that might occur if the identified risk materializes. The impact assessment can be quantified in terms of damage value (financial) to compare with predefined thresholds and determine the overall impact level on the organization. If the impact cannot be quantified in financial terms, the evaluator can consider other impact assessment criteria. The levels are defined as follows:

Status		Description
I1	Blue	Negligible Impact
I2	Green	Minor Impact
I3	Yellow	Moderate Impact
I4	Orange	Significant Impact
I5	Red	Disastrous Impact

Risk Rating

In risk assessment, a Risk Matrix must be established, which is derived from evaluating and categorizing the significance of risks based on their likelihood of occurrence and impact. Additionally, it should define the scope of acceptable risk levels, known as the risk appetite boundary.

Risk Rating = (Likelihood Assessment of events) X (Impact Assessment of events)

Risk Rating Table

Likelihood	Impact				
	1	2	3	4	5
5	(5)	(10)	(15)	(20)	(25)
4	(4)	(8)	(12)	(16)	(20)
3	(3)	(6)	(9)	(12)	(15)
2	(2)	(4)	(6)	(8)	(10)
1	(1)	(2)	(3)	(4)	(5)

The levels of risk are divided into 5 categories, which can be represented in a Risk Profile. The criteria for classification are as follows:

Risk Level Score	Risk Level	Description
20-25 scores	Extreme	For risks that are deemed unacceptable must be promptly managed to bring them down to an acceptable level. Immediate action is necessary to reduce the risk to within the organization's defined risk appetite.
10-16 scores	High	For risks that are deemed unacceptable, additional control measures must be established and closely monitored to ensure that the risk is reduced to an acceptable level.
6-9 scores	Medium	For risks that are considered acceptable but require control measures, these measures should be implemented to prevent the risk from escalating to a higher level. Responsibilities and clear timelines should be defined to ensure effective management and monitoring of these controls.
4-5 scores	Low	For risks that are deemed acceptable, they have only a minor impact on the organization. No additional management measures or control processes are required.

Risk Level Score	Risk Level	Description
1-3 scores	Insignificant	For risks that are considered acceptable and have no significant impact on the organization, no additional management measures are required, even if there are no control processes in place.

After receiving the assessment results, the risk management unit and the management department will proceed with the following actions:

- **Analyze and Summarize:** Use the Risk Profile to analyze and summarize the risk assessment results and prioritize the risk issues accordingly.
- **Present to Management:** Present the assessment results to the management to select key risk issues that need to be managed. Assign risk owners responsible for implementing additional risk management measures beyond those currently in place.
- **Report to Risk Committee:** Present the identified risk issues and the additional management measures to the Risk Management Corporate Governance and Sustainability Committee for their information.

4.5 Risk Response

Risk response involves developing a management plan to reduce risks to an acceptable level. Management may choose to employ one risk management method or combine several methods to decrease the likelihood and impact of potential events, ensuring that risks remain within the organization's acceptable level (Risk Appetite). The risk management approaches include:

1) **Risk Acceptance** involves acknowledging an existing risk without taking any further action because it is within the company's acceptable risk level. For risks that are not below the acceptable level but are still accepted by management, approval must be obtained from the company's board of directors.
2) **Risk Reduction** involves actions to decrease risk or find additional control methods to reduce the likelihood of an event occurring or to minimize the severity or damage of potential future events to an acceptable level for the organization. This can include designing internal controls, improving and correcting operational processes, and creating contingency plans.
3) **Risk Sharing** involves taking steps to mitigate the severity of risks by transferring or sharing part of the risk with external individuals or entities. This can include hiring

specialized external service providers, purchasing insurance, or diversifying investments. These actions help to reduce the remaining risk to an acceptable risk level.

4) **Risk Avoidance** involves stopping or canceling activities that generate risk. This approach is typically used when the risk is highly severe and no other risk response methods can sufficiently reduce the impact to an acceptable level.
5) **Risk Pursuance** involves continuing operations while accepting higher risks to achieve greater performance outcomes. This approach may involve adopting aggressive growth strategies. When choosing to accept these risks, management must understand the nature and extent of the necessary changes to achieve the desired performance outcomes, while ensuring that the risk level does not exceed the acceptable range.

Before establishing risk management strategies, executives must consider the following factors:

1) **Develop Risk Management Strategies:** Create strategies to reduce the impact and likelihood of risks to align with the company's acceptable risk level (Risk Appetite).
2) **Develop Detailed Risk Management Plans:** Outline the specifics of the risk management plans.
3) **Assign Risk Owners:** Designate individuals responsible for making decisions and implementing risk management plans.
4) **Approval and Endorsement:** Ensure that the risk management plans are approved and endorsed by the Risk Management Corporate Governance and Sustainability Committee.
5) **Implementation Responsibility:** Risk owners are responsible for executing the plans

4.6 Control Activity

Control activity are policies and operational procedures designed to ensure that risk management is effectively implemented in a tangible manner. These activities aim to manage risks to an acceptable level and prevent any adverse impact on the organization's objectives.

Control activities are tools for management to help the organization achieve its objectives. After determining appropriate risk management strategies, management will establish control activities to ensure that risk management is conducted efficiently and effectively. These control activities are divided into 3 (three) types:

Control Activities	Procedure
1. Preventive Control	It is an action to prevent events or errors from occurring in the first place, such as: • Segregation of Duties • Using passwords to limit access to information systems • Providing training
2. Detective Control	It is an action to identify activities, events, or errors that have already occurred to ensure appropriate corrective measures are taken, such as: • Data Confirmation • Account Reconciliation • Inventory counting • Error reporting
3. Corrective Control	It is an action to correct errors or damage that have occurred and prevent them from recurring in the future, such as: • Business continuity plans • Disaster recovery plans

4.7 Information and Communication

Information and Communication refers to the establishment of effective communication and information systems related to risk to ensure that executives and all employees understand the processes and their roles and responsibilities regarding risk management. This ensures the effective implementation of the risk management plan.

4.8 Monitoring

Monitoring is the process of tracking to determine whether the implementation is appropriate and whether risks are being managed effectively.

Risk management monitoring must be an ongoing activity and can be done in two ways:

1) Continuous Monitoring: This involves regular, consistent actions to promptly respond to changes and is considered part of regular operations.
2) Event-Based Monitoring: This is conducted after an event has occurred, allowing for quick resolution of any issues that arise.

The main objectives of monitoring are:

- To ensure that the risk management plan is implemented as specified.
- To evaluate the effectiveness of risk management and the consistency of control activities.
- To consider new risks or changes to existing risks in response to changes in the business environment.

Risks and risk control activities are constantly changing. Risk management plans or control activities that were previously effective may become less effective, or there may be neglect in implementing those control activities. Additionally, there may be changes in objectives or processes. Under these changes, management must regularly evaluate the risk management process to ensure that it remains effective.

Therefore, the company should support continuous proactive communication to monitor various issues, such as changes in risk levels, progress of risk management plans, or the effectiveness of risk management within the organization. Management might include monitoring as an agenda item in various meetings, such as executive meetings, working group meetings, monthly executive reports, risk management corporate governance and sustainability committee meetings. Continuous communication ensures that risk information is relevant, easily accessible, and can be used for timely decision-making. In some cases, informal communication channels may be more suitable. For example, for risks that need urgent management, discussing and reporting risks via phone might be preferred to make immediate decisions and manage risks promptly, avoiding delays that might occur through formal reporting channels.

After implementing the risk management framework, the company should regularly review and update the framework to align with business changes to ensure that controls remain effective. Factors related to the opportunities and impacts of risks, as well as the costs of managing risks, may change. Therefore, management should continuously review risks according to the 8-step risk management process.

Risk Management Framework 2026 Edition was approved by the Board of Directors Meeting No. 7/2025 on 14 Novembery 2025 and shall be effective from 1 January 2026 onwards.

- Signed -

Mr. Norachit Sinhaseni

Chairman of the Board

Central Plaza Hotel Public Company Limited