

# Risk Management Regulations

本文件內容為中鼎工程股份有限公司(中鼎)製作及所有之保密資料，受著作權等相關法令保護，僅中鼎員工得於其特定職務及契約義務之工作範圍內存取及使用，未經中鼎事先書面同意，不得將其中一部或全部重製、公開散布或洩漏予與業務無關之人。

The content of this document is CONFIDENTIAL information made and owned by CTCI Corporation (CTCI) and is protected by copyright laws and relevant laws/regulations. Only employees of CTCI are allowed to access and use this confidential information within the work scope under their specific and respective duties and obligations required by agreement which is not allowed to copy, reproduce, distribute publicly or disclose in whole or in part to any non-relevant person without CTCI's prior and written consent.

CONTENTS

	PAGE
RISK MANAGEMENT POLICY .....	2
1.0 Purpose .....	3
2.0 Scope .....	3
3.0 Definition .....	3
4.0 Responsibility .....	3
5.0 Activity .....	5
6.0 Supplementary Provisions.....	11

風險管理政策  
Risk Management Policy

## 宣言 (Declaration) :

本公司建立完善風險管控制度，有系統的因應及處置管控各種風險，並持續檢討修訂風險管理機制以提升風險管控成效，進而達成持續穩定成長及永續營運之目標。

CTCI Corporation has established a sound risk management and control system to systematically respond, treat and control various risks, and continue to review and revise the risk management mechanism to improve the effectiveness of risk management and control so as to achieve the goal of continuous and stable growth and sustainable operation.

## 說明 (Description) :

本公司風險管理之方式，係透過建構適當之企業風險管理制度，並將風險管理制度融入日常營運活動中，以有效管理本公司之經營風險。為此本公司將：

Through constructing proper risk management procedure, the risk management of CTCI Corporation will integrate into the daily operating activities to manage the operating risks effectively. For this purpose, CTCI Corporation will:

- 設立與公司策略一致之企業風險管理制度；  
Establish enterprise risk management system consistent with company strategy;
- 定義全體同仁在企業風險管理中所扮演之角色與權責，並與全體同仁溝通；  
Define the roles and responsibilities of all employees in enterprise risk management, and communicate with all employees;
- 擬定系統化的企業風險評估方式，以確認影響本公司之重大風險均被有效辨識；  
Prepare systematized enterprise risk assessment method to ensure that risks significantly affecting CTCI Corporation can be identified effectively;
- 確保企業風險相關之資訊透過明確且有效之管道傳遞；  
Ensure that information related to enterprise risk can be passed through explicit and effective channel;
- 整合企業風險管理機制於日常營運活動。  
Integrate enterprise risk management mechanism into daily operating activities.

企業風險管理為一持續之企業活動，瞭解並推行本公司風險管理制度為本公司全體同仁之職責。全體同仁應於其職務中善盡風險管理之職責，各級管理階層亦應以身作則，遵循本風險管理制度之相關要求。

Enterprise risk management is a continuous activity; all employees of CTCI Corporation are responsible for understanding and carrying out risk management system of CTCI Corporation. All colleagues shall properly perform the duty of risk management; each management level shall also comply with relevant requirements of this risk management system.



李銘賢 M.S. Lee  
總經理 President

## 1.0 Purpose

Risk management is an indispensable part when making a decision. CTCI Corporation's (hereinafter referred to as "the company") establishment of risk management mechanism to assist the employee to systematically identify and assess the risks in the daily operation, and further to take effective measure to manage such risks (or opportunity), so as to strengthen the operating quality and competitiveness of the company to pursue optimized efficiency.

The purpose of preparing this Risk Management Procedure (hereinafter referred to as "the procedure") is to:

- A. Describe the risk management procedure of the company, based on which the risks possibly encountered by each operating unit can be managed systematically.
- B. Provide principle of risk management, so that employees of the company can follow.

## 2.0 Scope

The procedure is applied to all of the company, and is the company's standard operating procedure and basic requirement on risk management. Each unit may prepare its risk management operation documents based on such basis as necessary in consideration of its individual business or operating characteristics, which can be referred to when employees are executing their works.

## 3.0 Definition

### 3.1 Risk

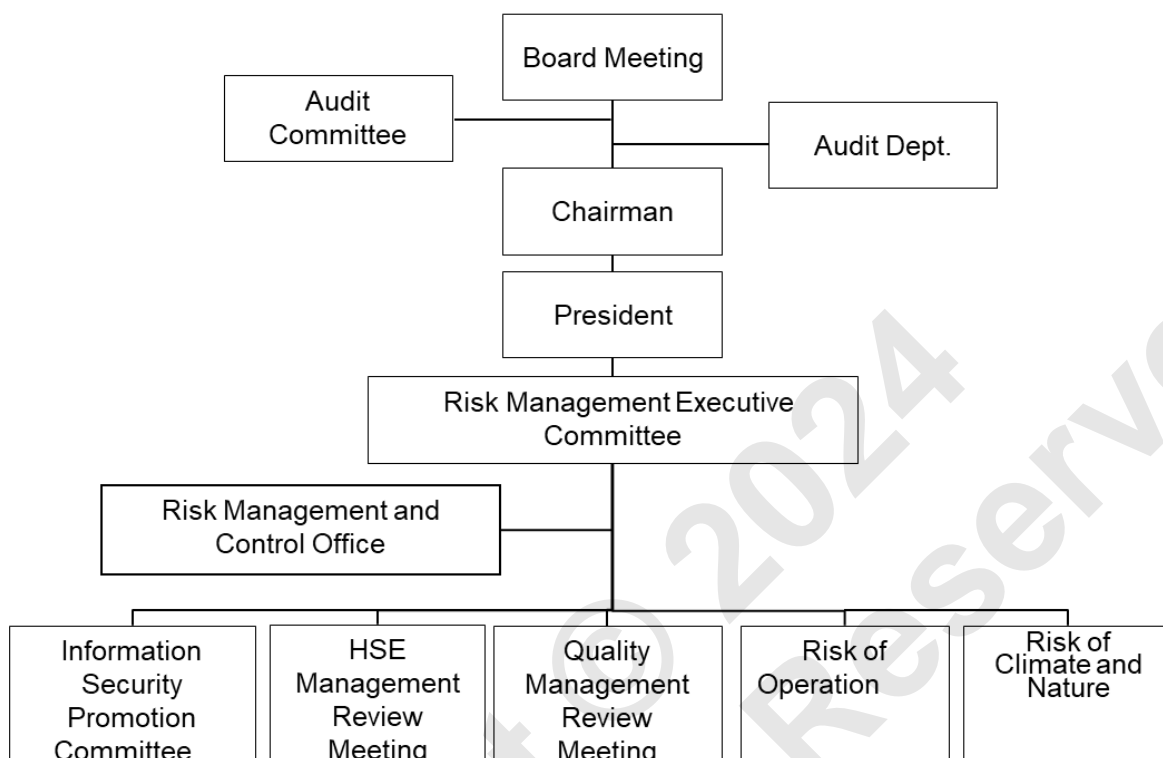
Risk means the probability of the internal issues, external issues, event, behavior or negligence obstructing the company's achievement of expected objective and strategy execution, or even threatening the existence of the company. Such event, behavior or negligence may cause adverse effect.

### 3.2 Interested party

Interested party is the person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity.

## 4.0 Responsibility

The risk management organizational structure is as follows:



#### 4.1 Risk Management Executive Committee

The Risk Management Executive Committee is the major monitoring mechanism for risk management of the company. The members mainly include President and Head of Executive Management Office and Business Operations. President is the Chairman of committee, and the convener is Chief Risk Officer.

- A. Approve risk management policy of the company;
- B. Examine risk management report and strategy of the company, and improvement plan.
- C. Supervise execution of risk control measure and improvement plan, communicate and deliver risk management affairs with and to all employees.
- D. Examine and assess the effectiveness of risk management measure and ask relevant unit to propose improvement plan.

#### 4.2 Each Unit

Head of each unit shall be fully responsible for risk management, their roles and responsibilities are as follows:

- A. Promote the supervision, identification and management of significant risks.

- B. Collect and monitor significant risk event of the division/department and evaluate the impact.
- C. report significant risk and relevant improvement plan to Head of Business Operations and provide a copy to the RCO.

#### 4.3 All employees

The implementation of daily risk management operation relies on continuous execution, their roles and responsibilities are as follows:

- A. Responsible for identifying the risks within the scope of daily works execution.
- B. Report to the supervisor immediately in case of a risk or an emergency risk event in responsible work.
- C. Comply with company policy, perform duty in accordance with the R&R, and implement relevant operations of risk management.

#### 4.4 Risk Management and Control Office (RCO)

- A. Establish and promote CTCI Group risk control management mechanism and culture.
- B. Regularly risk detection and control.
- C. Summarize and submit the risk management report, real time report and other works related to risk management.
- D. Promote and coordinate with activities related to risk management.
- E. Convene risk management review meeting.

#### 4.5 Audit Department

Audit Department makes and executes annual audit plan in accordance with the result of risk evaluation.

### 5.0 Activity

#### 5.1 Risk Management and Control Objective

In order to improve the effectiveness of risk control, the RCO shall consider the direction of risk control and the expected achievement, plan the annual risk management and control objectives, and shall be incorporated by Human Resources to annual KPI of the Head at all levels to enhance the



importance and effectiveness of risk control.

## 5.2 Regular Risk Management

### 5.2.1 Risk Management Process

The risk management process of the company is steps as stated in the following table:

Step	Item	Description
1	Risk Identification	Identify significant risk item
2	Risk Evaluation	Confirm overall risk rating by “the method of severity rating and probability index” or by “the method of Risk Quantitative Index”
3	Risk Response and Treatment	Pan the mitigations to address risks based on the risk control methods, and implement accordingly
4	Residual Risk Evaluation	Evaluate the rating of residual risk after completing the improvement plan
5	Improvement tracing	Progress tracing of improvement plan
		Evaluate effectiveness of improvement plan

### 5.2.2 Risk Identification

The risk items of the company can be identified through holding seminar. This seminar is convened by each division/department, participants thereof include division/ department Head, important leaders and other relevant employees. Each division/department may identify the risks through the following items:

- A. According to the annual objective; each division/department shall identify the risk items which may impact the achievement of objective;
- B. Each division/department shall identify the risk items might impact the internal value, culture, strategy, performance etc.;
- C. External factors, like legal, technology, market, social, cultural, environmental protection, etc. will impact the operation of the company;

- D. The expectation of interested parties will impact the company;
- E. Change of organization, process and management system will impact the company.

### 5.2.3 Risk evaluation

Risk evaluation can be done by “the method of consequence/probability matrix” or by “the method of Risk Index”).

#### A. The method of consequence/probability matrix

##### a. Evaluate Consequence Scale

Evaluate the consequence scale of each identified risk. The measurement of consequence scale is mainly stipulated according to the risk preference of the company, namely the risk of the company is willing to accept for the achievement of objective. The impact used by the company for measuring risk includes financial index and non-financial index. The impact of such risk will be stipulated according to the consideration of the impact on the “entire company”.

For definition of consequence scale, please see Attachment-01.

##### b. Evaluate Risk Probability

After the consideration of risk consequence scale, the probability scale shall be assessed simultaneously to determine the risk level. Please see below for the definition of risk probability.

Definition	Description
Frequent to occur	The event occurs under most circumstances. For example: it occurs at least once a month.
Very possible to occur	The event occurs upon negligence generally For example: it occurs at least once a quarter.
Possible to occur	Few opportunity for the event to occur For example: it occurs at least once a year.



Definition	Description
Not very possible to occur	Few opportunity for the event to occur For example: it occurs at least once per three years.
Extremely impossible to occur	The event is extremely impossible to occur For example: it will not occur within the coming three years.

c. Confirm Overall Risk Rating

Make the Risk Matrix according to the risk severity rating and risk probability index, then the company may determine the risk rating as below.

Consequence Probability	Extremely slight	Slight	Medium	Significant	Extremely significant
Frequent occurrence	<b>S</b>	<b>S</b>	<b>H</b>	<b>H</b>	<b>H</b>
Very possible to occur	<b>M</b>	<b>S</b>	<b>S</b>	<b>H</b>	<b>H</b>
Possible to occur	<b>L</b>	<b>M</b>	<b>S</b>	<b>H</b>	<b>H</b>
Not very possible to occur	<b>L</b>	<b>L</b>	<b>M</b>	<b>S</b>	<b>H</b>
Extremely impossible to occur	<b>L</b>	<b>L</b>	<b>M</b>	<b>S</b>	<b>S</b>

Note: H: High risk, S: Slightly high risk, M: Medium risk, L: Low risk.

d. The company shall periodically review the risk consequence scale and risk probability scale, and modify them to meet the requirement of internal and external issues, if necessary.

B. The method of Risk Index

When the consequence/probability matrix method cannot clearly evaluate the consequence and probability, the risk evaluation will be bias and lose the management function. To strengthen the practical and timeliness operation, the risk index method should be used for risk rating.

The definition and measurement of risk index are decided to evaluate the risk according to the experience of operation or the

expert suggestion. Risk Representatives will submit those definition and measurement to Risk Execution committee. After approved by Risk Execution committee, the index will be used to evaluate the risk. For example, the risk index of loss of talented people is the rate of resignation. The high risk is 20%, the slightly high risk is 15%, medium risk is 10% and low risk is 5% according to the experience and expert suggestion.

#### 5.2.4 Risk Response and Treatment

Each unit should plan the actions to address risks based on the risk control methods shown below:

- A. Terminate risk: terminate risk through stopping the execution of overall operation activity.
- B. Treat risk: take relevant actions, such as increase control, to reduce the impact or occurrence frequency of risk.
- C. Transfer risk: transfer risk through contracting risk related activity to the third party or insuring risk related activity.
- D. Tolerate risk: tolerate risk without taking any action.

Each unit should plan the actions to address risks based on the current risk rating. The actions for each risk rating should follow as below table. If the current risks are high risks or slightly high risks, the Improvement plan should be developed.

Risk Rating	Mitigation Planning
High Risk	<ul style="list-style-type: none"> <li>Establish the control procedure and requirement of measurement.</li> <li>Settle the Improvement targets and plans.</li> <li>Regularly review the effectiveness of the control method.</li> <li>Regularly report to Risk Management Committee.</li> <li>Check the source of the risk and necessary of existence.</li> </ul>
Slightly High Risk	<ul style="list-style-type: none"> <li>Establish the control procedure and requirement of measurement.</li> <li>Settle the Improvement targets and plans.</li> <li>Regularly review the effectiveness of the control method.</li> </ul>
Medium Risk	<ul style="list-style-type: none"> <li>Accept with conditions which need control procedures and monitor mechanism.</li> <li>Monitor the effectiveness of mitigation plans.</li> <li>Accept the current situation and continuously control by current procedure.</li> </ul>
Low Risk	<ul style="list-style-type: none"> <li>Accept the current situation and no need any action plans.</li> <li>Accept the current situation and continuously control by current procedure.</li> </ul>

#### 5.2.5 Residual risk evaluation

The residual risk is the expected rating of risk after completion of the improvement plan. The evaluating method is the same as current risks. The risk management representative of each unit shall initially determine the residual risk rating. After confirmed by Head of the unit, the residual risk rating can be the basis for management. For the unacceptable residual risk, further improvement plan shall be proposed.

#### 5.2.6 Improvement tracing and Report

Each risk unit shall continuously trace the execution of the improvement plan and evaluate the effectiveness of the improvement plan. If the effectiveness is not good, the improvement plan should be revised. Otherwise, the current risk rating should be gradually moved to lower level.

Risk management process should be done by each unit every half year. After the risk register is confirmed and signed to approve by the Head of the unit, the copy shall be transferred to RCO. RCO should review and report to the Risk Management Executive Committee.

### 5.3 Emergency Risk Event Treatment and Control

When an emergency risk event occurs and the action criteria are reached, the emergency risk event management and control mechanism shall be activated.

#### 5.3.1 Report

When risk event reached the action criteria, the event is a company-level risk event. The responsible unit shall immediately report to the BU Head.

#### 5.3.2 Establish an Emergency Risk Response Team

The responsible unit shall establish an emergency risk response team to treat risks. The responsible head of the emergency risk response team shall be recommended by the BU Head and approved by the President. After the emergency risk response team leader is determined, other team members should be summoned according to risk issues.

#### 5.3.3 Response, Treatment and Report

The emergency risk response team leader shall coordinate the treatment and control of risk events, and propose an emergency risk treatment plan, and report the latest risk treatment situation in writing weekly, bi-weekly or monthly. And according to the instructions or

control needs, hold meetings to report on the effectiveness of risk treatment. The report object shall go to the President; when the risk has been properly controlled, with consent, the case can be dismissed and closed.

#### 5.4 Risk Promote and Training

In order to enhance risk awareness and culture, management at all levels shall ensure that their subordinates understand the company's Risk Management Policy and the requirements of company's risk management and control, and then follow and implement them in daily operations.

The RCO should plan and conduct risk publicity and training activities every year to enhance the risk awareness of supervisors and colleagues.

#### 5.5 Reporting Frequency of Risk Management

The Risk Management Executive Committee shall report the status of risk management and control implementation to the Board of Directors every year.

### 6.0 Supplementary Provisions

The adoption and amendment of the Rules shall be approved by the board of directors' meeting.