

VIVOTEK INC.
Risk Management Policy

Approved by the Board of Directors on October 26, 2020
Amended and approved by the Board of Directors on July 29, 2024

- Article 1 Purpose
From a group-wide perspective, this Policy aims to mitigate and manage the various risks encountered in the Group's operations to levels that are within acceptable limits, using qualitative or quantitative methods for identification, assessment, control, supervision, and communication of potential risks. It serves as a foundational reference for strategic decision-making, ensuring the reasonable attainment of company strategic objectives.
- Article 2 Scope
This Policy applies to risk management operations across all levels within the Group.
- Article 3 Risk Management Organizational Structure
1. The Board of Directors of the Company serves as the highest governing body for risk management, overseeing the Company's compliance with laws and ensuring the implementation of comprehensive risk management. The Risk Management Committee supports the Board in supervising the execution and effectiveness of risk management.
 2. The General Manager acts as the chief executive responsible for risk management. Department heads, business unit managers, and regional managers serve as frontline risk managers, tasked with detecting, identifying, assessing risks, and developing corresponding strategies. They regularly review and supervise these activities during operational meetings.
 3. The General Manager establishes crisis response teams for different types of risks as events arise, assigning relevant managers to coordinate responses.
 4. The audit unit is responsible for auditing the implementation of the internal control system.
- Article 4 Risk Management Responsibilities
1. Roles of the Board of Directors and the Risk Management Committee:
 - (1) Approve risk management policies, procedures, and frameworks.
 - (2) Ensure alignment of risk management policies with operational strategic directions.
 - (3) Supervise the establishment of appropriate risk management mechanisms and foster a risk management culture.
 2. Role of the Chief Risk Officer
The Chief Risk Officer shall understand the various impacts of the different types of risks on the Company and ensure the effectiveness of risk management, bearing ultimate responsibility for it.
In managing risks, the Chief Risk Officer not only focuses on risks to individual units but also considers the cumulative effects of various risks to the Company's overall perspective. They facilitate interdepartmental risk management interactions and communication.
 3. Role of the Risk Management Unit

Department heads, business unit managers, and regional managers act as frontline risk managers, with the following main responsibilities:

- (1) Ensure timely and accurate transmission of risk information.
- (2) Ensure effective implementation of risk regulations within relevant units.
- (3) Assess changes in the external environment and internal policies to determine risk categories and propose appropriate response strategies.

Article 5 Risk Management Process

To strengthen the functionality of risk management, the Company employs processes including risk identification, assessment, control, supervision, and communication. This ensures a comprehensive understanding of each risk's scope and the implementation of appropriate measures to effectively manage them, efficiently allocating limited resources to relevant risk management tasks.

1. Risk Identification: To effectively manage various risk factors, the Company identifies risks in the following areas:

- (1) Strategic:
 - i. Industry changes
 - ii. Technological changes
 - iii. Business model formulation
 - iv. Organizational adaptability
- (2) Operational:
 - i. Market demand and capacity expansion
 - ii. Business continuity risks (including operational interruptions like supply chain disruptions and production halts)
 - iii. Information security
 - iv. Supply chain management
 - v. Intellectual property
 - vi. Customer concentration
 - vii. Corporate reputation
 - viii. Talent acquisition, retention, and development
 - ix. Strategic investments
- (3) Financial:
 - i. Interest rates, exchange rates, inflation
 - ii. Taxation
 - iii. Credit
 - iv. Liquidity
 - v. High-risk/high-leverage financial investments, derivative trading
- (4) Hazard Events:
 - i. Climate change
 - ii. Occupational health and safety

- iii. Fires or other man-made disasters (including hazardous substance use in products and processes)
- iv. Natural disasters
- (5) Regulatory Compliance:
 - i. Environmental regulations (including carbon pricing, energy taxes, renewable energy regulations, etc.)
 - ii. Antitrust, anti-corruption, and fraud prevention
 - iii. Personal data protection
- 2. Risk Assessment:

Business unit managers, department heads, and regional managers analyze and identify risks defined within the scope of risk management. After identifying potential risk factors, they assess the likelihood of risk events occurring and the potential negative impact they could have. This analysis helps understand the impact of risks on the company and serves as the basis for risk management.
- 3. Risk Control and Supervision:
 - (1) Risks related to daily operational activities of each unit are managed by the responsible units.
 - (2) Significant crisis events involving multiple departments or plant areas undergo cross-departmental or cross-plant risk assessments. The General Manager or designated personnel are responsible for commanding and coordinating these efforts, identifying feasible strategies for crisis prevention and establishing crisis response procedures and recovery plans.
 - (3) Changes in organizational responsibilities for various risk factors listed in Appendix I do not require approval from the Board of Directors.
 - (4) Any deficiencies identified during risk supervision and control should be reported through normal channels as per regulations.
- 4. Risk Communication:
 - (1) In addition to provisions stipulated in these regulations, the Company's risk management operations adhere to internal control regulations and relevant policies and procedures of supervisory authorities.
 - (2) The Chief Risk Officer or designated personnel report annually on the Company's risk management operations to the Risk Management Committee and the Board of Directors.

Article 6

Implementation

This Policy took effect after having been submitted to and adopted by the Board of Directors. Subsequent amendments thereto shall be put into effect in the same manner.

The first amendment was made on July 29, 2024.

Appendix I

Risk Types	Risk Factors	Responsibility Unit
Strategic	Industry changes	General Manager
	Technological changes	General Manager
	Business model formulation	General Manager
	Organizational adaptability	General Manager
Operational	Business continuity risks (including operational interruptions such as supply chain disruptions and production interruptions)	Operations Division, Business Units
	Information security	IT Division
	Supply chain management	Operations Division
	Market demand and capacity expansion	Operations Division
	Intellectual property rights	Intellectual Property Department
	Customer concentration	ODM Business Division, Brand Business Division
	Corporate image	Global Marketing Division
	Talent attraction, retention, and development	Human Resources Department
Financial	Strategic investments	Office of the General Manager
	Interest rates, exchange rates, inflation	Finance Department
	Taxation	Finance Department
	Credit	Finance Department
	Liquidity	Finance Department
Hazard Events	High-risk/high-leverage financial investments, derivative transactions	Finance Department
	Climate change	CSR Team
	Occupational health and safety	Occupational Safety Team
	Fires or other man-made disasters (including hazardous substance use in products and processes)	Occupational Safety Team, Plant Manager
Regulatory Compliance	Natural disasters	General Affairs Department
	Environmental regulations (including carbon pricing, energy taxes, renewable energy regulations, etc.)	General Affairs Department
	Antitrust, anti-corruption, and fraud prevention	Office of the General Manager
	Personal data protection	IT Division