



Delta Electronics, Inc.
Delta Group Risk Management Policy
(Translation)

Passed by the Board of Directors on July 29, 2020

Article 1 (Purpose)

The purpose of the Delta Group Risk Management Policy ("Policy") is to reduce various risks to a tolerable and controllable range through identification, assessment, control, monitoring and communication of potential risks from the perspective of Delta Group ("Group") by qualitative or quantitative management methods, as well as to provide a reference for developing operational strategies. The Policy has been formulated in order to achieve the Group's strategic goals in a reasonable manner.

Article 2 (Scope)

The Policy shall be applicable to risk management operations at all levels of the Group.

Article 3 (Organization of Risk Management)

- A. The CEO is the highest authority in the field of risk management, and COO and heads of each business group (BG Heads), heads of each functional unit (Function Heads) and heads of each region (Region Heads) are responsible for frontline risk management to perform their duties for risk detection, identification, assessment and development of risk response strategies. They shall review and monitor risk in a regular manner in strategy meetings.
- B. For different types of risks, the CEO shall form risk response teams for different events, and designate personnel to be responsible for overall coordination.
- C. From the perspective of the internal controls system, the internal audit department is responsible for auditing the implementation of risk management.

Article 4 (Responsibility for Risk Management)

- A. The role of the highest authority of risk management
The highest authority of risk management shall recognize the impact of different types of risks on the Group and ensure the effectiveness of risk



management. The ultimate responsibility for risk management rests with the highest authority.

B. The role of risk management units:

The COO, BG Heads, Function Heads and Region Heads are responsible for frontline risk management, and their main responsibilities are as follows:

- a. To ensure the delivery of risk information in a prompt and accurate manner.
- b. To ensure that risk management shall be effectively implemented within a unit.
- c. To determine the risk factors and suggest response plans according to the changes in the external environment and internal strategies.

Article 5 (Procedures of Risk Management)

To implement a sound risk management mechanism, the following procedures of risk management, including risk identification, risk assessment, risk control, risk monitoring and communication, apply to each risk factor and the formulation of action plans towards appropriate risk management and efficient resource allocation.

A. Risk Identification:

To control all risk factors, the Group has identified the following risk factors:

- a. Strategic
 - i. Changes in industry
 - ii. Changes in technology
 - iii. Establishment of business models
 - iv. Responsiveness of organizational structure
- b. Operational
 - i. Market demand and capacity expansion
 - ii. Business continuity operation (Business interruption risk including supply chain disruption or production disruption)
 - iii. Information security
 - iv. Supply chain management
 - v. Intellectual property rights
 - vi. Customer concentration
 - vii. Corporate image
 - viii. Talent attraction, recruitment and training of personnel



- ix. Strategic investment
 - c. Financial
 - i. Interest rate, foreign exchange rate and inflation
 - ii. Taxation
 - iii. Credit
 - iv. Liquidity
 - v. High-risk and/or highly leveraged financial investments, derivative transactions
 - d. Hazardous Events
 - i. Climate change
 - ii. Occupational safety and health
 - iii. Fire or other man-made disaster (inclusive of restriction of hazardous substances in products or manufacturing)
 - iv. Natural disaster
 - e. Compliance
 - i. Environment regulations (inclusive of carbon pricing, energy tax, renewable energy regulations, and others.)
 - ii. Antitrust, anti-corruption and fraud
 - iii. Personal data protection
- B. Risk Assessment:
- Business groups, functional units and regions shall analyze and identify risk factors within the scope of risk management defined by the Group. By analyzing the degree of negative impact and the likelihood of occurrence of risk events, the Group shall realize the impact of the risk and set a basis for risk management.
- C. Risk Control and Monitoring
- a. Risks generated from daily operations shall be controlled and monitored by relevant operation units based on their nature.
 - b. For crisis events involving cross-departments or cross-plants, the CEO or the person designated by CEO shall be responsible for direction and coordination to identify feasible strategies to prevent crisis events and formulate crisis management procedures and recovery plans.



- c. A table of department responsibility for each risk factor is provided in Appendix 1. Any adjustment due to organization changes of the table set forth in Appendix 1 needs not be approved by the Board of Directors.
 - d. Any deficiency found in risk control and monitoring should be reported through normal channels pursuant to relevant policies.
- D. Risk Communication
- a. Unless otherwise provided by the Policy, risk management of the Group shall follow the Group's internal control policies and the applicable regulations shall be promulgated by the competent authority.
 - b. The highest authority for risk management or the person designated by the highest authority for risk management shall report the implementation of the Group's risk management to the Board of Directors once a year.

Article 6 (Implementation)

The Policy shall be implemented subject to the approval of the Audit Committee and the Board of Directors. Subsequent amendments shall be effective in the same manner.