Chicony Power Technology Co., Ltd.
2024 Operational Status of Risk Management Policies and Procedures

Risk Management Policies and Systems

To strengthen corporate governance, implement comprehensive operational risk management, and ensure the integrity of the Company's risk management framework, the Board of Directors approved the "Risk Management Policies and Procedures" on August 5, 2011. These serve as the highest guiding principles for risk management across the entire organization.

Scope of Risk Management

Risk management across all levels of the Company covers operations, finance, environment, hazard incidents, and climate-related business activities. Processes for identifying, assessing, monitoring, and reporting risks are adjusted as necessary in response to changes in the business environment.

Roles and Responsibilities in Risk Management

1. Board of Directors

The Board is the highest authority responsible for the Company's risk management. Its responsibilities include ensuring legal compliance, promoting and implementing overall risk management, maintaining visibility of risks that may impact operations, and ensuring the effectiveness of management mechanisms.

2. Audit Office

The Audit Office reports directly to the Board as an independent unit responsible for conducting internal audits. Its duties include reviewing internal control deficiencies, operational efficiency, and providing recommendations for improvement to ensure the continual effectiveness of internal controls. Audit findings serve as a basis for system enhancements.

3. General Manager

The General Manager serves as the convener of the Company's risk management program, coordinating implementation across all departments. Responsibilities include evaluating risks associated with operational decisions, promoting response strategies, handling media relations and external communications, and managing human resource allocation.

4. Finance Center

Responsible for assessing financial risks.

5. Information Technology Division

Responsible for information security management, ensuring the confidentiality, integrity, and availability of corporate information assets, maintaining regulatory compliance, and reducing operational risks.

6. All Operational and Administrative Units

Each unit supervisor is responsible for conducting risk identification and control in daily operations, implementing company-wide risk awareness, and regularly executing preventive measures to keep risks within acceptable levels.

Implementation Status

1. The Board of Directors approved the Company's Risk Management Policies and Procedures in August 2021.
2. Each executing unit identifies risks and proposes control strategies and actions (as detailed below).
3. The Audit Office supervises implementation to ensure the effectiveness of employee awareness and execution of risk management.

Risk Categories, Potential Risks, and Control Strategies

1. Climate Risk

Potential Risks

- Increasingly extreme weather conditions: natural disasters, water shortages, and power outages, which may impact production.

Control Strategies and Actions

- Coordinate with local governments to secure priority status for power and water supply at each plant.
- Invest in disaster prevention measures and conduct regular maintenance.
- Assess risks associated with raw material suppliers' geographic locations.
- Implement energy management systems in each plant and evaluate the feasibility of renewable energy installations.
- Install flood prevention and drainage systems at all factories and establish emergency response procedures.

2. Environmental Risk

Potential Risks

- Global temperature rise (increase in greenhouse gas emissions).

Control Strategies and Actions

- Conduct greenhouse gas inventories and undergo third-party verification; Taipei HQ, Dongguan, Suzhou, and Chongqing plants have completed ISO 14064 verification.
- Establish Science Based Targets (SBT). Reduction targets were approved in August 2022. Taipei HQ and all plants continue to execute energy-saving and carbon-reduction measures.
- Increase R&D investment in high-efficiency products to reduce product carbon emissions.
- Increase the use of environmentally friendly materials in products to reduce non-recyclable waste generation.

3. Occupational Safety and Health (OSH) Risk

Potential Risks

- Workplace safety risks for employees.

Control Strategies and Actions

- Taipei HQ, Dongguan, Suzhou, Chongqing, and Thailand plants have all obtained ISO 45001 occupational safety and health certification.
- EHS teams at HQ and plants conduct regular onsite inspections to reduce hazards.
- Conduct workplace environmental monitoring to ensure no adverse health impacts on employees.

4. Fire and Explosion Risk

Potential Risks

- Hazards from soldering irons, heat guns, hot-melt glue guns, and other high-temperature equipment.

Control Strategies and Actions

- Established safe-use regulations for soldering irons and high-temperature equipment; regular training is provided to raise risk awareness.
- Implemented soldering iron registration and accountability system to ensure proper maintenance and storage.
- For high-temperature devices without automatic cooling, require installation of auto power-off timers and protective covers to prevent accidental contact.

5. Employee Health Management

Control Strategies and Actions

- Expanded senior employee health screenings: in 2024, high-level health check packages previously limited to supervisors were extended to employees with over five years of service (once every three years).

- Conduct health monitoring and follow-up for high-risk employees.
- Perform regular environmental disinfection to maintain workplace hygiene.
- Provide influenza vaccination.
- Promote healthy workplace certification.

6. Information Security Risk

Potential Risks

- System anomalies
- External cyberattacks and malicious intrusions

Control Strategies and Actions

- Maintain ISO 27001 information security certification annually.
- Implement firewalls, antivirus programs, and cloud ATP (Advanced Threat Protection) for email security; IT staff perform regular testing to build comprehensive defense mechanisms.
- Block abnormal connections by monitoring web access to external sites.
- Conduct quarterly firewall and internal network vulnerability scans and perform remediation.
- Strengthen disaster prevention, monitoring, reporting mechanisms, incident management, disaster recovery drills, and backup procedures.
- Conduct quarterly cybersecurity awareness training to enhance employee vigilance.

7. Financial Risk

Potential Risks

- Foreign exchange fluctuations.

Control Strategies and Actions

- Offset USD receivables and payables naturally to reduce exposure.
- Monitor global economic conditions and exchange rate trends for any remaining net USD positions or future cash flows.
- Execute forward foreign exchange contracts at appropriate times for hedging.