Risk Management Status Report in 2025

2025/11

Procedures and Implementation of Risk Management

1 Identification and Definition of Risks

Identify the sources of material that may affect the company's strategies and organizational goals as well as the causes and potential consequences of such risks and events.

Financial risk

Exchange and interest rates.

Environmental and carbon reduction risks

Climate Change, Environment, and Occupational Safety

Information security risk

Information security.

Strategy and operational risks

Strategy development and operation, Technologies, Capital expenditures, and Raw material price and supply chain

Corporate sustainability Risks

Legal compliance, Manpower management, and Corporate Image

NEW

2 Risk Measurement

Analyze the identified risks' probabilities and their impacts to consider control and management measures by factoring in past experiences.

Management units

Such units shall fully understand the risks facing the businesses they are responsible for to have relevant risk management mechanisms factored into respective operation management regulations。

Implementation units

Such units shall abide by and carry out necessary operations and risk management processes to ensure the risks involved are controlled and bearable。

3 Risk Analysis and Assessment

Risk Measurement Matrix

Assess risk levels by focusing on the material risks and events of the company's concern based on the levels of financial and/or reputational impacts on the company and the probabilities of occurrence.

Review

Risk Impact × Probability = Risk Exposure

Supervision

Scale of Severity of Risk Consequences

Extremely Slight	Slight	Medium	Significant	Extremely Significant

Vigilance Standard: Significant

Action Standard: Extremely Significant

Risk Appetite (Risk Tolerance): Extremely Slight, Slight, Medium

Risk Tolerance: Extremely Slight, Slight, Medium, Significant

NEW

4 Risk Control and Management

Action Plan

Engage in comprehensive monitoring throughout risk changes and developments to accordingly adjust risk response strategies.

Major Risks Throughout the World and Asia Pacific

			Risk Level	Risk Trend	Corresponding Risk Categories at Walsin Lihwa
Capital and Credit Markets	world	Volatility in global financial markets, rising credit pressures, and a weakening real estate market are increasing risks for the banking and credit markets.	Rising	Unchanged	Financial risk
	Asia	Tightening financing channels and rising borrowing costs will further worsen the outlook for low-credit issuers.	High	Unchanged	
Economic recession	Asia	China's economic slowdown, coupled with excessive industry competition and weak consumer confidence, continues to amplify downward pressures.	High	Unchanged	Strategy and Operational Risks
Tariffs and Trade	world	Tariff and trade tensions are suppressing economic growth and driving inflation.	↑ Very High	Unchanged	Strategy and Operational Risks
	Asia	Tariff uncertainties are reshaping regional supply chains and delaying capital expenditures, while trade diversion and rising protectionist pressure intensify market disruptions.	↑ Very High	Unchanged	
Geopolitics	world	Geopolitical tensions and disruptions to transportation routes in the Middle Eastern straits are affecting supply chains and commodity markets, weakening investment confidence and capital expenditure.	High	Worsening	Strategy and Operational Risks
	Asia	Escalating conflicts in the Middle East and the South China Sea are disrupting supply chains, worsening cost and investment conditions, and heightening risk-aversion sentiments.	↑ High	Worsening	
ESG	world	Increasing climate risks and the lack of consensus on net-zero pathways are elevating the risks associated with the energy transition.	Rising	Worsening	Environmental and Carbon Reduction Risks
	Asia	Extreme weather events and setbacks in the energy transition are raising the costs of net-zero decarbonization and inflationary pressure, posing threats to investment and social stability.	Rising	Worsening	
Information Security	world	Cyberattacks and rapid technological change pose potential threats to global business operations and government infrastructure.	Rising	Worsening	Information Security Risk
	Asia	The rapid advancement of technology and escalating cyberattacks are disrupting business models and undermining credit profiles.	Rising	Unchanged	

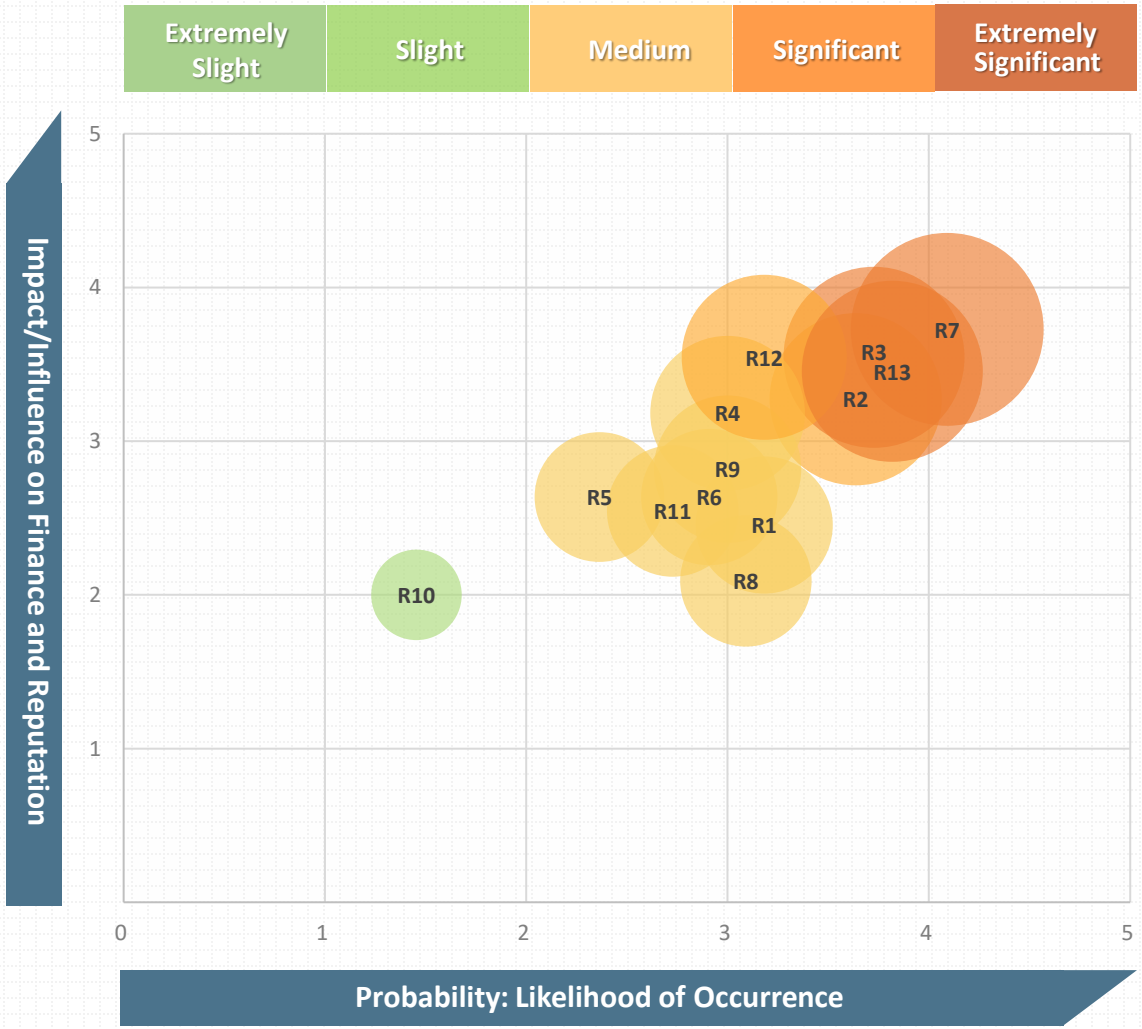
Note: Taiwan Ratings identified the major risks in Asia Pacific in the 3rd quarter of 2025 to commence a one-year follow-up of such risks.

Identification of Emerging Risks

Identification of emerging risks is based on the Global Risks Report 2025 released by the World Economic Forum and resilience under pressure as noted in Global Credit Conditions Q3 2025 published by Taiwan Ratings and S&P Global) Ratings while factoring in Walsin Lihwa's business development and future outlook planning.

Emerging Risks	Description	Potential Impact
Geoeconomic confrontation increases operational and strategic risks.	The uncertainty of global political and economic dynamics has heightened geoeconomic risks. In particular , a potential "Trump 2.0" trade war may trigger higher tariffs and further regionalization of supply chains. The growing adoption of tariff-based protectionist measures by various countries is expected to add additional operational risks and complexity.	Geoeconomic rivalry may lead to tariff barriers that disrupt the Company's operational planning, resulting in market contraction or operational shocks. If the Company is unable to promptly adjust its overall strategies and supply chain deployment, it may face reduced operational flexibility and an increased risk of profit margin compression. Over the long term, such conditions may erode the Company's competitive advantage and market share.
Operational and Strategic Risks Arising from Increased Cybersecurity Threats and Improper Use of Technology Driven by Artificial Intelligence	Artificial intelligence (AI) and cloud services enhance operational efficiency but also introduce significant cybersecurity challenges. AI models may be affected by training data bias or adversarial attacks, compromising information security and the accuracy of decision-making. Cloud services face risks such as insufficient data access control, supplier security vulnerabilities, and DDoS attacks, which may result in confidential information leakage or system paralysis. Hackers may also infiltrate the organization by attacking software suppliers and implant malware into the Company's systems, leading to large-scale cybersecurity incidents.	If AI-generated outputs are not verified, they may result in misinformation, reduced reliability, and decreased operational precision. Meanwhile, employees may find it difficult to determine whether the data they input into or obtain from AI systems involve trade secrets or sensitive information, exposing the Company to heightened risks of information leakage and infringement. Improper use of AI may increase the likelihood of confidential or proprietary information being disclosed, weakening the Company's information confidentiality, damaging its reputation and credibility, and ultimately undermining its competitiveness.

Risk Matrix



Risk Categories		Risks in 2025
Finance	R1	Rising financing costs and reduced financial flexibility
	R2	U.S. stagflation concerns increasing exchange rate uncertainty and volatility risks
Environment and Carbon Reduction	R3	**Escalating climate change issues and lack of consensus on net-zero pathways increasing transition risks**
	R4	Operational disruptions at facilities due to the growing impact of extreme weather events
Information Security	R5	Frequent and sophisticated malicious cyberattacks, with increasingly deceptive phishing techniques
	R6	Heightened cybersecurity risks driven by artificial intelligence, raising the likelihood of trade secret leakage
Strategy and Operation	R7	**Geoeconomic confrontation and tariff protectionism creating economic barriers and worsening investment conditions**
	R8	Growing demand for new product development in green energy applications and manufacturing services
	R9	Employee recruitment and retention-wise, labor shortages make it difficult to recruit suitable employees.
Corporate Sustainability	R10	Occurrences of bribery, corruption, or other violations of professional ethics
	R11	Emerging sustainability regulations across countries increasing compliance uncertainty and operational costs
Energy	R12	Energy transition requirements and energy shortages driving the need for diversified energy deployment
	R13	Rising energy prices (e.g., natural gas and electricity) pushing up long-term operating costs

Risks and Control Measures

Emerging Risks

Categories	Probability of Occurrence	Degree of Impact	Control Measures
Intensifying climate change and the progressive tightening of global decarbonization requirements	High	Medium-High	1. Increase the awareness of and disclose the company's carbon reduction target, strategy, and tangible action plan. 2. Strengthen the implementation of effective carbon reduction, expedite green power procurement planning, and analyze the operational impact from carbon fees and taxes as well as green power procurement. 3. Report regularly to the Board of Directors to guide and oversee decarbonization and energy-transition plans, ensuring that sustainability issues are integrated into operational decision-making. 4. Implement IFRS Sustainability Disclosure Standards by establishing climate-related disclosure processes and data inventory mechanisms to enhance the quality and transparency of climate-related information.
Rising energy prices driving long-term increases in operating costs	High	Medium-High	1. Introduce automation and high-efficiency equipment to optimize production processes, improve energy utilization efficiency, and reduce operating costs. 2. Install renewable energy systems—such as solar power—at production sites to increase energy self-sufficiency and reduce reliance on purchased electricity. 3. Conduct regular reviews of energy consumption and carbon emissions to drive energy-saving and emission-reduction actions and promote the adoption of high-efficiency technologies. 4. Mitigate the impact of energy price volatility and enhance product competitiveness through low-carbon processes and participation in carbon-trading mechanisms.
Geoeconomic confrontation increasing operational and strategic risks	High	**Very High**	1. Strengthen the company's resilience to regionalized economic challenges through global deployment, thereby enhancing critical manufacturing capabilities and operational flexibility. 2. Establish cross-regional production and distribution capabilities for both the Stainless Steel and Wire & Cable Businesses — diversifying the risks arising from tariff barriers and policy uncertainties, while reducing exposure to single-market disruptions. 3. Deepen the European Stainless Steel Business's presence in key sectors — such as aerospace and energy — to expand high-end product applications and service offerings.
AI increasing cybersecurity risks and raising the likelihood of trade secret leakage	Medium	Medium	1. Establish an AI-enabled proactive threat detection and defense system — including the implementation of cloud-to-edge Zero Trust architecture and the launch of OT/industrial control system cybersecurity protection — to support the Company's "Digital Sustainability" objective. 2. Continuously enhance employees' cybersecurity awareness by conducting regular social engineering drills, enforcing incident reporting procedures, and strengthening response capabilities through ongoing exercises. 3. Strengthen information security policies and management frameworks by building an integrated cybersecurity protection platform, implementing technical safeguards, and participating in external cybersecurity rating assessments to achieve both internal and external compliance requirements. 4. Develop a cybersecurity governance roadmap aligned with international standards, reinforcing information security risk management to ensure the confidentiality, integrity, and availability of trade secrets and sensitive information.

Cybersecurity Risks and Management Measures

Expanding AI Automation Deployment

1. Establish Azure cloud security detection (MDx), endpoint detection and response (EDR), and remote access control (SASE).
2. Implement intelligent server protection (DS) and user behavior analytics (UBA).
3. Deploy Security Copilot as an intelligent cybersecurity assistant (bot).

Information Security Management and Technical Protection Measures

1. Achieved early certification of ISO 27001:2022 and revised over five internal regulations and control procedures.
2. Established office printing management and privileged access management mechanisms.

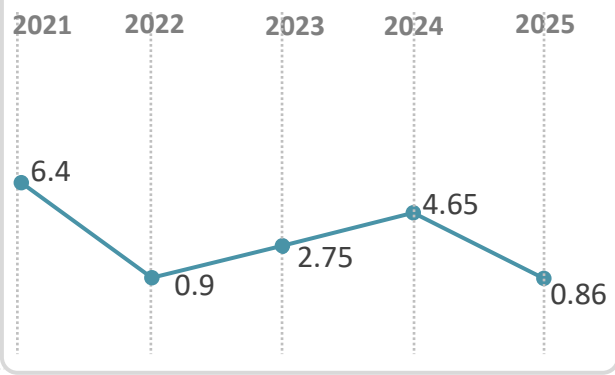
Cybersecurity Awareness and Training Programs

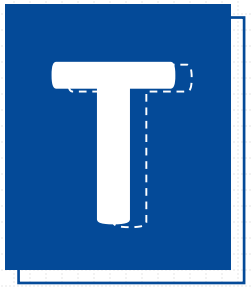
1. Incorporated cybersecurity awareness and security guidelines into mandatory annual employee training and included them as a performance appraisal bonus item.
2. Held an annual Cybersecurity Awareness Month, publishing 10 awareness articles.
3. Issued regular cybersecurity bulletins to communicate company policies and new knowledge, accumulating over 12 awareness articles.

Social Engineering Drills and Cybersecurity Incident Reporting Exercises

1. Conducted company-wide and spear-phishing social engineering drills once every two months.
2. Held annual cross-departmental cybersecurity incident response exercises, engaging 27 employees and 14 external vendors.

Employees Hooked in Social Engineering Drills





Thank you