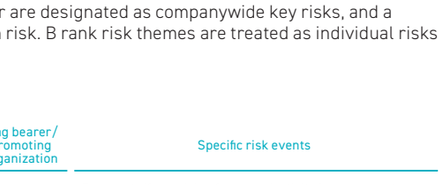
# Response to Companywide Key Risks

Resonac has organized the Risk Management Committee chaired by the CEO. The Committee facilitates cross-organizational deliberations by senior executives on the risk management system, key risks facing the Group, and countermeasures for addressing them. Companywide key risk themes were identified based on the deliberations of the Risk Management Committee, at a senior executives study session held in June 2024, and reviewed annually at a senior executives study session held in March 2025.

| Monitoring level* | 2025 companywide key risks themes |
|---|---|
| S | ① AI x Talent: Restructuring of the talent portfolio due to the rise of AI<br>② Country risks, economic security<br>③ AI-driven technological innovation, risks arising from market changes<br>④ Capital investment delays: Advancement and automation delays New<br>⑤ Supply chain management (SCM) issues A rank ▸ S rank |
| A | ① Information leak, cyberattacks<br>② Misconduct and corruption, compliance scandals<br>③ Environmental regulatory risks<br>④ Human rights risks |
| B | ① Unpredictable markets<br>② Industry restructuring<br>③ Quality issues<br>④ Aging facilities<br>⑤ Lack of IT Infrastructure<br>⑥ International tax<br>⑦ Interest rate fluctuation |

* S rank: The most significant risks to the Company's operations
A rank: Significant risks to the achievement of Company's targets
B rank: Significant risks to business operations

2025 companywide key risk heat map

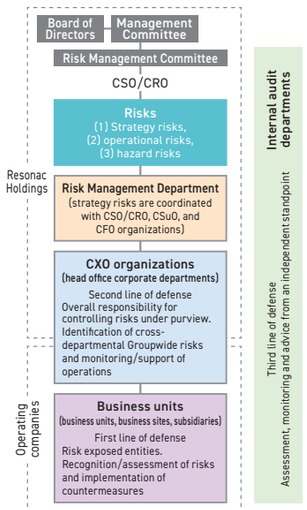



Resonac's risk management system was resolved by the Board of Directors as a key function of the internal control system, and a reporting and monitoring system is established. Our Group's Risk Management Rules are designed to comprehensively and individually address management risks affecting our business. In these rules, we have established executive bodies and responsible departments and provided for management methods that comply with ISO 31000 and other standards.

In implementing risk countermeasures, we have established a comprehensive risk assessment process that combines bottom-up companywide risk identification and top-down companywide key risk identification activities, and approaches risks from both on-site and management perspectives, creating a system that reflects changes in the external environment.

In the companywide key risk heat map analysis, risk themes ranked A or higher are designated as companywide key risks, and a promoting organization is selected to act as the "flag bearer" for addressing each risk. B rank risk themes are treated as individual risks and are addressed by each organization.

## Risk management system




## Companywide key risks

| Rank | Companywide key risks themes | Risk classification | Flag bearer/ promoting organization | Specific risk events |
|---|---|---|---|---|
| S | Restructuring of the talent portfolio due to the rise of AI | Human resources / labor | CHRO | ・Excess staffing arising from productivity improvements<br>・Obsolescence of employees' existing skills |
| S | Country risks, economic security | Accidents, disasters | CSO/CRO | ・Increased risk of a decline in sales, supply chain disruptions, and market access restrictions due to national interest first policies by each country<br>・Increased employee safety risk and asset confiscation, production suspension/delay, and business suspension/delay risks due to military clashes |
| S | AI-driven technological innovation, risks arising from market changes | Management (business investments) | CTO | ・Impact on our business operations from changes in competitiveness and market environments due to the spread of AI |
| S | Instability of supply chains | Procurement, logistics | CMEO/CQO | ・Export restrictions imposed by a country that supplies raw materials, cutting off access to those materials |
| A | Information leak, cyberattacks | Information management | CDO (IT Supervisor) | ・Theft of cutting-edge technology information, customers' personal information, etc., and shutdown of production and core systems due to ransomware infection, etc.<br>・Intentional exfiltration of confidential information by an insider |
| A | Misconduct and corruption, compliance scandals | Compliance | CSuO | ・Damage to corporate value due to impact from the transaction suspensions and reputational damage caused by loss of trust from stakeholders due to the occurrence of compliance violations |
| A | Human rights risks | Management (sustainability) | CSuO | ・Loss of business opportunities due to delayed response to regulations: Impact from suspension of shipments and distribution to Europe due to delayed response to new regulations, mainly in Europe |
| A | Environmental regulations, sustainability | | | |



For each companywide key risk theme, we conduct a risk scenario analysis and take preventive measures. For country risks identified as S rank, we identify priority regions and businesses by analyzing sales, and then continuously monitor external environmental risks in cooperation with CXOs and business units and work to minimize risks by promotion of establishing production and supply systems based on local production for local consumption.

## Example: Risk dashboard for country risks

| Rank | Companywide key risks themes | Flag bearer organization | Risk events | Monitoring index (KRI) |
|---|---|---|---|---|
| S | Country risks | CSO/CRO | Turmoil in global markets due to accelerated economic security policies by the U.S. and China | Foreign and industrial policies by the U.S. and China |

**"Supply chain instability" risk scenario**

**Risk events:** Increased risk of sales declines and supply chain disruptions, etc., due to the acceleration of economic security policies by the U.S. and China (national protection and domestic industry development policies)

**Types of policies to watch**

Protection policies:
- (1) Import tariff hikes
- (2) Acceleration of restrictions on resource imports and exports
- (3) Tightening of export restrictions related to cutting-edge semiconductors
- (4) Revisions to trade agreements

Development policies:
- (5) Support for domestic industries and national policies promoting domestic production

**Risk scenario events to watch**

| Impacted areas | Risk scenarios impacting our industry |
|---|---|
| U.S., China, and others | A retaliatory tariff battle between the U.S. and China triggered by the U.S. tariff hikes as well as the trend spreading to other countries. |
| Global | Export and sales restrictions on important minerals accelerate as part of dual-use restrictions. |
| China | Export restrictions on China are expanded to include not only semiconductors and their manufacturing equipment and technology, but also semiconductor materials. |

**Main impacts on the Company**

- A: Declining price competitiveness of export products (especially to China and the U.S.), declining sales, and restructuring of supply chains in various countries
- B: Procurement of raw materials (especially from China) is disrupted, making it impossible to continue production*
- C: Decrease in export sales to China

| Response measures and plans | Preventive measures (normal times) | Ex-post measures |
|---|---|---|
| | ●Continued monitoring of external environmental risks in cooperation with CXOs and business units (geopolitical risks, Trump 2.0 status, etc.)<br>●Minimization of risks by establishing a production and supply system based on local production for local consumption<br>* Identify purchase items with high procurement risk and implement measures | Form response teams within relevant departments to discuss and implement actions to be taken. |

## Examples of measures in progress

● Companywide distribution of a country risk report

● Formulation of Taiwan contingency evacuation plan

- ●Implement officer simulation
- ●After reaffirming that human safety is the top priority, the decision was made to formulate an evacuation plan

In progress
- ●Personnel evacuation policy (creation of an action workflow in tense situations)
- ●Gathering information in the event of an emergency
- ●Transfer of authority to local subsidiaries

## Security incident that occurred at Resonac

Minoru Nomaru
Chief Digital Information Officer (CDIO)

In the early morning of May 20, 2025, we experienced an incident in which files on Resonac Group servers and PCs were encrypted. Subsequent investigations confirmed that it was caused by a cyberattack using ransomware, and we established an emergency response team to respond swiftly to the incident. To prevent damage from spreading, we immediately took action, such as tentatively disabling internal networks, which resulted in some computer systems becoming unusable and business operations being halted. We then launched a detailed investigation with the cooperation of external experts. We also filed a police report, cooperated with relevant government ministries and agencies, and continued to take various actions to minimize business impact on all customers and business partners.

As a result of our emergency actions, by July 4, we confirmed that there was no impact on product shipments. Furthermore, an external cyber security expert team analyzed the ransomware and concluded that there was no risk of infection spreading to customers' and business partners' network from our network.

We sincerely apologize for the great concern and inconvenience this incident has caused to our business partners and related parties.

We have confirmed that the cause of this incident was an external attacker who somehow infiltrated the our internal network and activated the ransomware. We will thoroughly implement measures to prevent similar incidents from occurring in the future.

**May 20, 2025**
1. External attacks were detected on some of our servers, and ransomware infection was confirmed.
2. Immediately begin an investigation with the cooperation of external experts and establish an emergency response team to take swift action.

**June 9**
Transition to a task force centered on CDIO

**July 4**
External experts analyzed the ransomware and concluded that there is no risk of infection spreading between our network and our customers' networks.

We aim to establish a system capable of responding promptly to incidents within the next 1.5 years. Furthermore, within three years, we aim to establish a sophisticated security framework to predict and detect advanced threats beyond ransomware.

**Emergency measures** | **Short-term measures in 2025 and long-term measures in 2026 and after**