



Risk type	Risk description	Management measures
 <p>Cybersecurity risk</p> <p>Network attacks and protection of business secrets</p>	<ul style="list-style-type: none"> The Company's website, Internet portal, and employees' access to the Internet or the mail system all present vulnerabilities for computer viruses and Trojan horses, which may cause disruptions to the Company's operations. Employees may be unaware of their obligations to protect internal business secrets acquired through work, which results in business secrets being handed to other employees that do not have authorized access. This occurrence is especially likely among the staff of the Company's managers and insiders, and any leaks of information currently under development may result in losses of competitiveness, missed opportunities to surpass competitors, or even manipulation of share prices, posing compliance risks. 	<ul style="list-style-type: none"> Kaori introduced a new cybersecurity officer position in 2022, whose responsibilities are to evaluate cybersecurity requirements and allocate resources with an administrative and governance mindset. Kaori has made plans to obtain certification for ISO 27000 Information Security Management System, expecting to execute the project in 2023 and pass certification in the 4th quarter. To avoid network attacks, the Information Technology Department not only outsources management of the Company's website to an external service provider in coordination with the Public Relations Department, but has also adopted the use of a new-generation firewall to replace the conventional firewall and antivirus combination. The Information Technology Department even introduced the latest XDR hack prevention technology, implemented triple backups for critical data (local/cloud/off-site), developed an HA infrastructure for important systems, and added a hyper-converged infrastructure (HCI) on top of the conventional VM environment to create a dual infrastructure that ensures the ability to recover from disasters. Kaori implements cybersecurity control from three different perspectives: system, policy, and management. Despite the fact that the Information Technology Department has implemented robust systems and policies and is actively promoting awareness, it is up to the management to take effective disciplinary actions to ensure compliance from employees and thereby deter any potential losses of business secrets.
 <p>Change of corporate image and crisis management</p> <p>Corporate reputation</p>	<ul style="list-style-type: none"> Risk of damage to business reputation due to certain decisions or commercial practices 	<ul style="list-style-type: none"> Risk of damage to business reputation due to certain decisions or commercial practices

Internal Audit and Correction

Kaori has implemented internal controls in accordance with the “Regulations Governing Establishment of Internal Control Systems by Public Companies” and the competent authority's instructions, and taken steps to ensure that they remain effective at supporting the operational goals of the Company. Annual audit plans and special audits are organized as requested by the competent authority or the Board of directors or as suggested by the management.

The Company has an Audit Office that carries out audit tasks according to the annual audit plan and on specific issues. Findings are compiled into official reports and distributed to the respective auditees. The Audit Office executed audit tasks according to Kaori's audit plan and issued a total of 61 audit reports in 2022 (subsidiaries in China were audited by way of document review due to COVID-19). These reports were distributed to the respective auditees. All audit reports were presented to the Audit Committee for review and reported in Board of directors' meetings. For any defects or abnormalities discovered during the audit, the auditee will be instructed to rectify or make improvement plans, and progress will be tracked on a quarterly basis until improvements have been made.

2.5 Compliance

Compliance is the most fundamental requirement in business management. For the protection of stakeholders' interests and for the continuity of business operations, Kaori has established internal policies in accordance with the laws of relevant authorities and enforced them to serve as guidance for business decisions. Kaori did not commit any anti-competitive, anti-trust, or monopolistic practices in 2022, nor did it suffer financial losses due to violations or lawsuits concerning anti-competitive behavior.

Management System

1. Corporate governance aspect

- Functional committees have been assembled to supervise financial performance and internal control within the Company. Furthermore, corporate governance guidelines and Board performance assessments have been implemented to enhance the Board's supervisory role over important decisions, their ability to offer professional opinions, and increase the level of information transparency.
- Kaori observes TWSE's corporate governance evaluation and corporate governance best practices as guidelines for improving corporate culture and compliance.

2. Personnel aspect

- Development of integrity rules and regular audit
Ethics and compliance are the foundation of business integrity; at Kaori, we enforce these values through policy implementation, self-evaluation, whistleblowing, and whistleblower protection. The management leads by example and requests every employee to observe laws and internal policies that are relevant to their duties. Compliance is examined through yearly internal control self-assessment; the outcomes are reviewed by the Audit Office. The Audit Office executed audit tasks according to Kaori's audit plan and issued a total of 61 audit reports in 2022 (subsidiaries in China were audited by way of document review due to COVID-19). Kaori has established a set of guidelines that employees must obey when conducting business activities. All employees are required to duly comply with the "Business Integrity Code of Conduct" regardless of their role, rank, or location and to compete for business in an honest, fair, and compliant manner that supports Kaori's corporate culture.
- Regular education and training
Kaori provides employees with a variety of training options based on the types of duties assumed to keep them informed about business ethics and compliance requirements. Orientation, classroom courses, internal seminars, and external training are some examples of the training offered.

3. Environmental safety and health aspect

Policies and measurements have been implemented to ensure that all business activities, products, and services comply with occupational safety, health, and environmental regulations. Meanwhile, performance of the environmental management system is monitored so that effective corrective and preventive measures can be taken in a timely manner.

Assessment System

Kaori has several effective controls in place to ensure compliance. The Company checks new regulatory amendments on a monthly basis and conducts compliance audits on all plant sites on a yearly basis. Kaori did not commit any violations of safety, health, environmental protection, or fire safety rules in 2022. There were, however, two incidents where the Company had violated or failed to comply with applicable laws, for which it was fined a sum of NT\$236,333. Both incidents have been improved upon according to the instructions of the competent authority. Aside from the above, no major compensations or losses were reported in annual internal audits.

Item No.	Description	Amount of loss (NT\$)
1	Land-related dispute: Removal of superficies located on the odd lot land in the rear part of Zhongli 1st Plant at No. 204-2, Zhonggong Section, Zhongli District	131,996
2	Violation of building regulations: With regards to the expansion of the Kaohsiung Plant, Kaori was found to have demolished or constructed factory facilities without prior approval, without timely reporting/inspection, and without change of design schematics, and was fined as a result	104,337