Corrective Process Against Negative Impacts | Risk Management

GRI 2-12,16,25/403-2

Policy (our fundamental view)

Recognizing the various risks surrounding the NOF Group, we promote risk management initiatives with the aim of preventing the occurrence of loss risks and minimizing their impact when they do occur, thereby contributing to the achievement of management strategy targets.

1. The NOF Group comprehensively identifies various management risks surrounding its business, and conducts risk assessments based on the impact and frequency of each factor in order to identify risks that need to be addressed as a priority.
2. According to the characteristics of the identified risks, We work to minimize the impact on management by taking appropriate measures to reduce the impact of risks that have materialized, as well as measures to reduce the probability of occurrence.
3. We work to objectively verify the effectiveness of risk countermeasures by periodically conducting risk assessments, while working to recognize and evaluate new risks.
4. Under the leadership of the Risk Management Committee, we promote the risk management of the NOF Group by implementing the above risk management cycle.

Organizational setup

The Risk Management Committee, the Compliance Committee, the RC Committee, and the Quality Management Committee analyze management risks, consider countermeasures, and report to the Board of Directors. The Board of Directors receives reports and deliberates as necessary on various business risks, including those related to compliance, information management, and environment and safety, as well as confirmation and evaluation of the comprehensiveness of risks. We manage and monitor Group companies in accordance with the rules on the management of Group companies, and offer advice, as necessary; while any important matters that are deemed to materially impact our subsidiaries' assets or profit and loss are approved by the NOF Board of Directors or the Executive Committee.

Risk assessment process

We prepare a list of risks in consideration of the business characteristics of each department and the environment surrounding the business, including global political, economic, and social conditions. We also send a questionnaire to each NOF site and Group company. Based on the results of the questionnaire, the manager of each department conducts a risk evaluation and estimates the impact and frequency of occurrence of each risk in the NOF Group based on the results of the evaluation. Based on the results, a risk map is prepared in a workshop of directors and operating officers to confirm critical risks and select priority risks to be addressed.

Flow of risk assessment

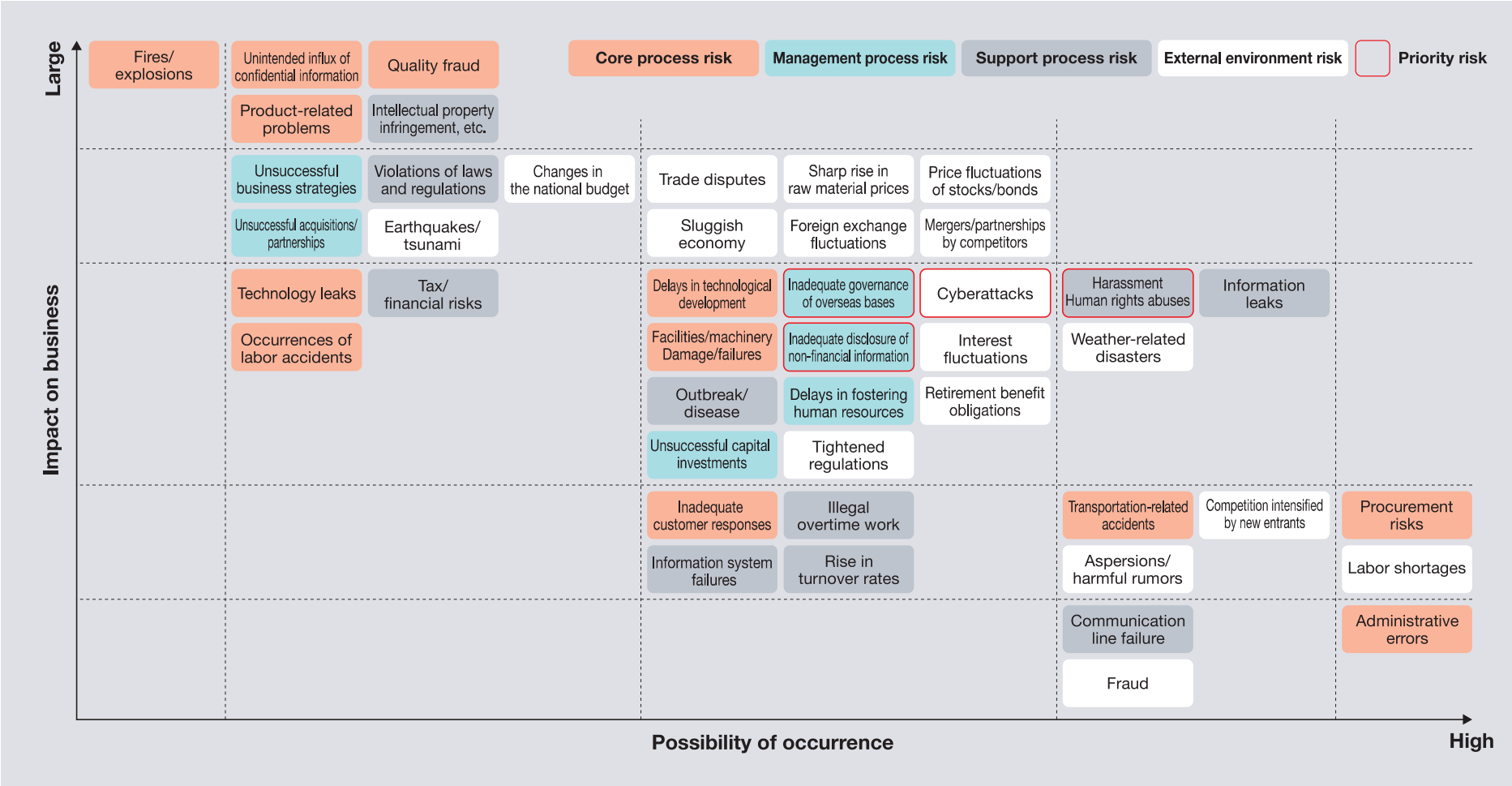
- Expected risks of the NOF Group are identified and a list of risks is prepared
- With regard to the list of risks, managers of each department conduct a risk evaluation based on the questionnaire
- The questionnaire results are aggregated and an evaluation is conducted for the impact and frequency of occurrence of risks to the NOF Group
- Directors hold discussions based on the aggregated results, and confirm the evaluation of the impact and frequency of occurrence of each risk
- A risk map is prepared for the entire NOF Group based on the evaluation of the impact and frequency of occurrence of each risk
- The major risks in the risk map are confirmed
- The priority risks are identified based on countermeasure status

Corrective Process Against Negative Impacts | Risk Management

GRI 2-12,16,25/403-2

Risk Map (excerpt)

The risk map is prepared based on the results of the risk evaluation at the directors' workshop. The risk map is revised and priority risks are identified on a yearly basis in order to implement activities aimed at enhancing the NOF Group's resilience.



Corrective Process Against Negative Impacts | Risk Management

GRI 2-12,16,25/403-2

Overview of priority risks and status of countermeasures

Priority risks	Risk description	Ongoing countermeasures
Harassment / human rights abuses	Possible decline in trust in the Company due to human rights abuse, such as abuse of authority and sexual harassment at workplaces	• Establish the Code of Ethical Conduct and the Compliance Manual • Establish a consultation service with male and female employees as well as a contact point with attorneys
Cyberattacks and information system failures	Possible information leaks and interruption of business activities, due to illicit access from outside such as cyberattacks and information system failures	• Develop an information security management system by establishing the information security management rules and appointing a person responsible for information security management, etc. • Develop a defense system against illicit access and implement safety measures at appropriate, rational levels
Inadequate governance of overseas bases	Possible decline in trust in the Company due to fraud, such as violations of laws and regulations, as a result of inadequate governance at overseas bases	• Develop a system for ensuring the appropriateness of business operations • Request a regular report on the state of business execution and financial conditions, etc.; conduct business audits
Inadequate disclosure of non-financial information	Possible loss of trust from stakeholders due to uncertainty about economic and environmental impact as well as social reputation	• Analyze the current situation and identify targets • Establish management indicators and targets and develop specific measures

Overview of major risks and status of countermeasures

Major risk	Risk description	Ongoing countermeasures
Technology leaks	Possible decline in the NOF Group's competitiveness, due to leakages of technical information, and similar products/technologies provided by competitors	• Establish rules for trade secrets • Develop a management system for trade secrets • Strengthen information security training for employees
Raw material procurement	Risk of social credibility falling due to human rights violations such as forced labor and child labor, or procurement of raw materials suspected to damage the environment	• Statement of compliance with the CSR Procurement Policy and CSR Procurement Guidelines in sales contracts • Ongoing supplier surveys through various questionnaires
Occupational accidents and incidents	Possible casualties among employees and neighborhood residents, possible suspension of business activities, and possible compensation for damages as a result of large-scale fires and explosion accidents at plants	• Continuously improve health and safety levels through Responsible Care activities • Strengthen the system for conducting safety assessments at the time of new construction • Formulate emergency response manuals and implement trainings • Implement joint disaster prevention drills and dialogue activities with local municipalities
Quality fraud	Possible decline in trust in the Company due to quality fraud, falsification of quality inspection results, and other situations	• Ensure strict management of data related to quality control • Raise awareness and train employees
Intellectual property infringement, etc.	Possible compensation for damages and possible orders to suspend manufacturing and shipment, due to infringements of intellectual property rights	• Develop a check system for intellectual property management and patent infringement • Educate employees on intellectual property including patents and trademarks
Violations of laws and regulations	Possible suspension of business activities and possible payments of surcharge, etc. following administrative dispositions taken in response to violations of laws and regulations, such as the Unfair Competition Prevention Act, Antimonopoly Act, Subcontract Act, Foreign Exchange and Foreign Trade Act, Chemical Substances Control Act, and Pharmaceutical and Medical Device Act	• Prepare a Global Compliance Manual and country-specific compliance manuals based on the legal systems of each country • Establish compliance training and contact points for whistle-blowing/consultation • Establish a system for disseminating information on revisions to laws and regulations
Earthquakes, tsunami, infectious diseases	Possible interruption of production activities or business activities, including sales and distribution, due to earthquakes, tsunami, or other natural disasters	• Formulate a business continuity plan (BCP) • Conduct BCP training and internal audits • Implement flood countermeasures for critical facilities
Delays in fostering human resources	Possible stall in development of core human resources who will be responsible for business growth, due to non-functional mid- to long-term human resources training plans	• Build a system for deliberation and evaluation of company-wide human resources development policy plans • Build a system to oversee progress and results related to human resources development

Information security management

(1) Management of trade secrets and protection of personal information

NOF considers information assets as an important management resources in corporate activities, and the establishment of secure information assets are essential for achieving stable management, thus, we have established the Information Security Policy as a basic principle for promoting effective utilization and protection of information assets. At the same time, based on the recognition that protecting personal information is a fundamental social responsibility, NOF has established and published the Privacy Policy.

Under such policies, NOF has set forth specific measures for enhancing the levels of confidentiality, completeness, and availability of information and specific ways of handling personal information in its internal rules and manuals and is ensuring thorough dissemination and understanding within the company.

Such internal rules and manuals include: 'Information Security Management Rules', 'Personal Information Protection Rules', 'Provisions Related to Information Systems', 'Information Equipment Handling Manual', and 'Confidential Information Handling Manual'.

Information assets: Information obtained from customers and business partners, trade secrets of NOF Group and personal information, and systems for utilizing such information

(2) Management structure

In the organizational aspect, the Information Security Management Subcommittee is set up to deliberate and make decisions on important matters related to information security. Under 'Information Security General Manager', who is the chairperson of the Subcommittee, 'Document Information Security Manager', 'Electronic Information and Information System Security Manager', 'Personal Information Complaint Handling Manager', as well as a person responsible for management at each division, production base and department are appointed to administer the implementation of specific measures.

Against threats such as unauthorized access from outside, information leakage, tampering, and destruction, appropriate and reasonable security measures are implemented. In addition, NOF continually reviews and strives to improve the information security management and personal information protection systems and measures through internal audits.

NOF Group Information Security Policy

The NOF group considers information assets as an important management resources in corporate activities, and the establishment of secure information assets are essential for achieving stable management, thus, our group shall establish and comply following policies.

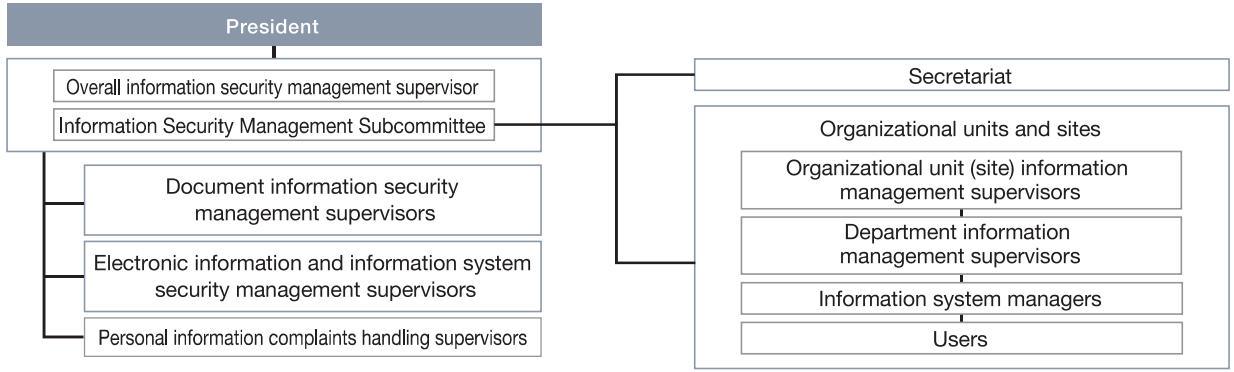
Information assets: Information obtained from customers and business partners, trade secrets of NOF Group and personal information, and systems for utilizing such information

1. The NOF Group shall develop the information security system to further strengthen the management function of information assets.
2. In order to protect the information assets from leakage, falsification, and destruction, the NOF Group shall provide information security education for employees, develop regulations, and implement technical measures for information systems.
3. The NOF Group shall comply with laws, regulations, codes and contractual obligations related to information security.
4. In the event of an information security incident, the NOF Group shall respond promptly and appropriately to each incident and prevent a recurrence.
5. The NOF Group shall maintain and continually improve these efforts in this Policy.

Corrective Process Against Negative Impacts | Risk Management

GRI 2-12,16,25/403-2,4

Diagram of NOF's information security management system



Risks and opportunities in information security and measures against risks

Risks and opportunities	Details	Measures
Risks	● Long-term stoppage of production, sales, and R&D activities and loss of corporate credibility due to cyberattacks (illicit access, malware infection) ● Loss of corporate trust and technological competitiveness due to leakage of confidential and personal information	● Conduct self-inspections, develop improvement plans, and implement improvement plans ● Information sharing through meetings of IT managers of domestic Group companies (once a year) ● Conduct training on handling suspicious emails (once a year) ● HDD encryption for computers taken outside the company, and restrictions on the use of private storage media ● Conduct information security-related training for employees (once a year)
Opportunities	● Improvement of company competitiveness through cybersecurity measures ● Earning of customer trust and enhancement of corporate brand value by strengthening information asset management ● Increased employee awareness through strengthened information security	-

Promotion of the Business Continuity Plan (BCP*)

NOF has formulated a BCP, to enable its core business to be continued or, if damaged, to be restored quickly while minimizing the loss of business assets in the event of a natural disaster such as an earthquake or tsunami, or an emergency situation such as the COVID-19 pandemic. The activities of the BCP Task Force to promote the BCP primarily focus on the formulation of the BCP manual which sets forth the responses to be implemented in normal times and in emergencies, in addition to the preparation and yearly renewal of information on the estimated damages to the plant and various government-, infrastructure- and supply chain-related information, which will be required when resuming operations. Additionally, the BCP Task Force performs annual internal audits and training in an effort to firmly establish the BCP and to enhance its effectiveness.

In fiscal 2023, as a response to information security risks, we conducted BCP training based on the assumption of a cyberattack, and confirmed the initial response procedures in the event of an incident and the roles of each department and site for business continuity. The training was designed to minimize damage in the event of a cyberattack and to improve response capabilities, including speediness.

* Abbreviation for Business Continuity Plan. The BCP illustrates policies, systems, and procedures designed to prevent important operations from being interrupted even in the face of unforeseen events, such as a major earthquake or other natural disaster, the spread of infectious disease, a terrorist incident, a major accident, a disrupted supply chain (supply network), or a sudden change in our business environment, and, if business is interrupted, that it is restored within the shortest possible timeframe.