Corrective process against negative impacts | Risk management

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

Our fundamental view

1. The NOF Group comprehensively identifies various management risks surrounding its business, and conducts risk assessment based on the impact and frequency of each factor in order to identify risks that need to be addressed as a priority.
2. 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. 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 Control Committee analyze management risks, consider countermeasures, and report to the Board of Directors. The Board of Directors conducts integrated assessment of 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. The risks are deliberated at the Board of Directors as necessary.

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.

Confirming "major risks" and identifying "priority risks"

The NOF Group works to comprehensively identify management risks surrounding the Group, considering the characteristics of each business as well as external environments, including political, economic and social changes. In addition, we evaluate the impact and the frequency of occurrence of each identified risk on Group management, confirming major risks and taking appropriate measures against risks identified as "priority risks," which necessitate enhanced resilience.

Moreover, for other risks, each committee evaluates the current response, sorts it into categories such as "retained" and "reduced," and considers additional countermeasures as necessary.

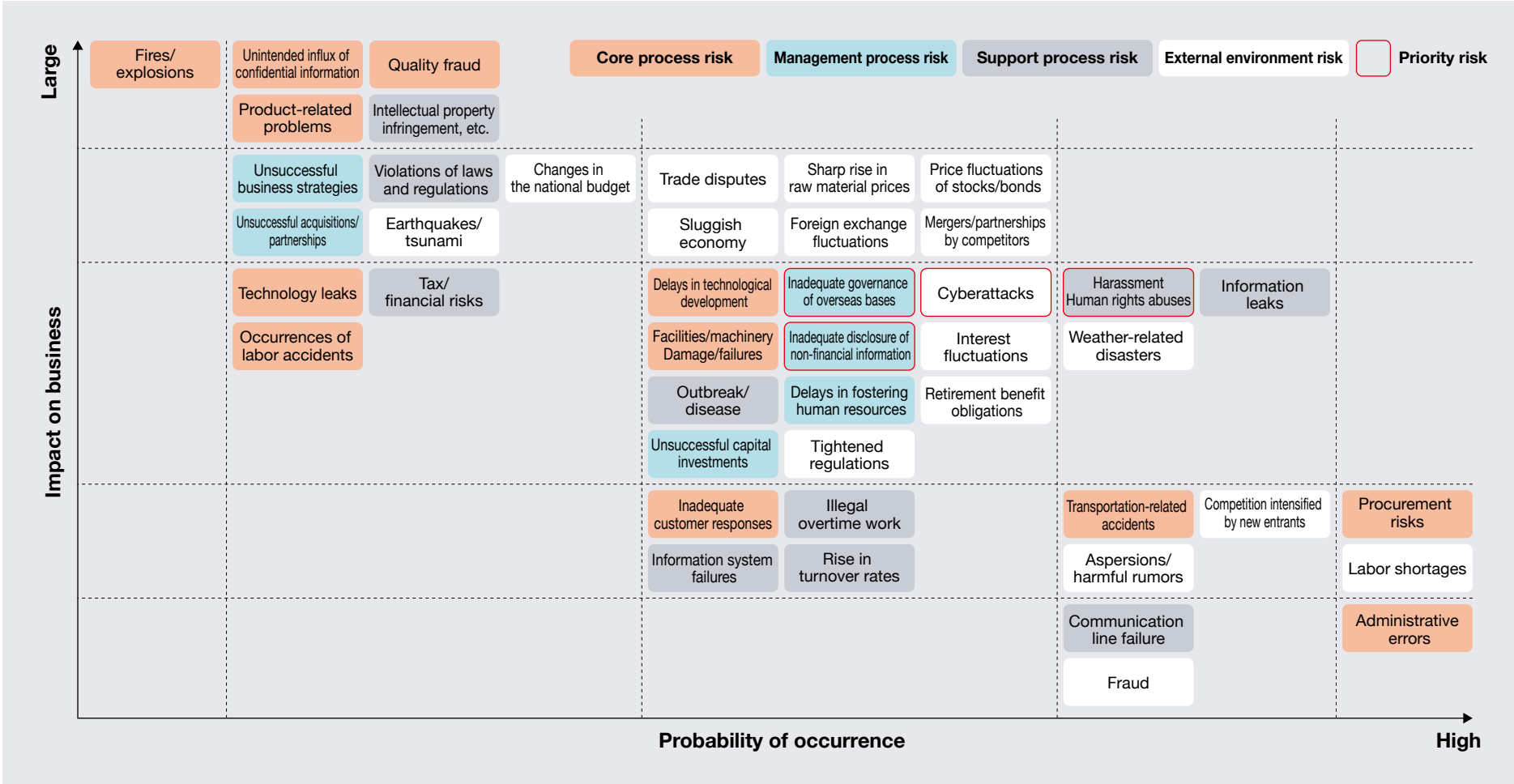
Flow of risk assessment

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 major risks and status of countermeasures (excerpt)

Major risk	Risk description	Ongoing countermeasures (excerpt)
Earthquakes/tsunami	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) • Implement internal audits and training regarding the BCP
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
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 condition, etc.; conduct business audits
Cyberattacks Information system failures	Possible information leaks and interruption of business activities, due to illicit access from outside such as cyberattacks and information system failures	• Establish the information security management rules and appoint a person responsible for information security management, etc. • Develop a defense system against illicit access and Implement safety measures at rational levels
Fires/explosions	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	• Formulate emergency response manuals and implement trainings • Implement joint disaster prevention drills and dialogue activities with local municipalities
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
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
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
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 an external contact point with attorneys
Delays in fostering human resources	Possible stall in development of human resources who will be responsible for the growth of the NOF Group, due to a failure of medium- and long-term human resource development plans	• Promote rank-specific trainings for next-generation human resources for specific issues • Promote/foster international human resources and human resource rotation
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

Corrective process against negative impacts | Risk management

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

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.

Information security management

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

Recognizing the importance of information as one of our vital management resources to business activities and the indispensability of active strengthening of corporate competitiveness by active utilization of information and firm establishment of information security to steady business management, NOF has set forth the Information Security Policy as a basic principle for promoting effective utilization and protection of information. At the same time, recognizing protection of personal information as its obvious social responsibility, NOF has formulated and announced the Privacy Policy.

Under such policies, NOF has set forth specific measures for enhancing the levels of confidentiality, completeness, and utility of information and specific ways of handling personal information in its internal rules, including information security management rules, personal information protection rules, and information system-related sets of provisions, a confidential information handling manual, and an information equipment handling manual, and is ensuring their thorough understanding by the staff.

(2) Management setup

In the organizational aspect, the Information Security Management Subcommittee is set up, and under its chairperson, who has overall supervising responsibility for information security management, persons responsible for document information security management, electronic information and information system security management, and addressing complaints regarding personal information, as well as a person responsible for management at each level of organizational unit, are appointed to administer the implementation of specific measures. Against illicit access from outside and other risk factors including loss, destruction, and alteration, safety measures are taken at appropriate and rational levels. In addition, NOF continually reviews through internal auditing setups and measures pertaining to information security management and protection of personal information to improve them wherever necessary.

* The BCP (acronym for Business Continuity Plan) 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.