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 assessment 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.

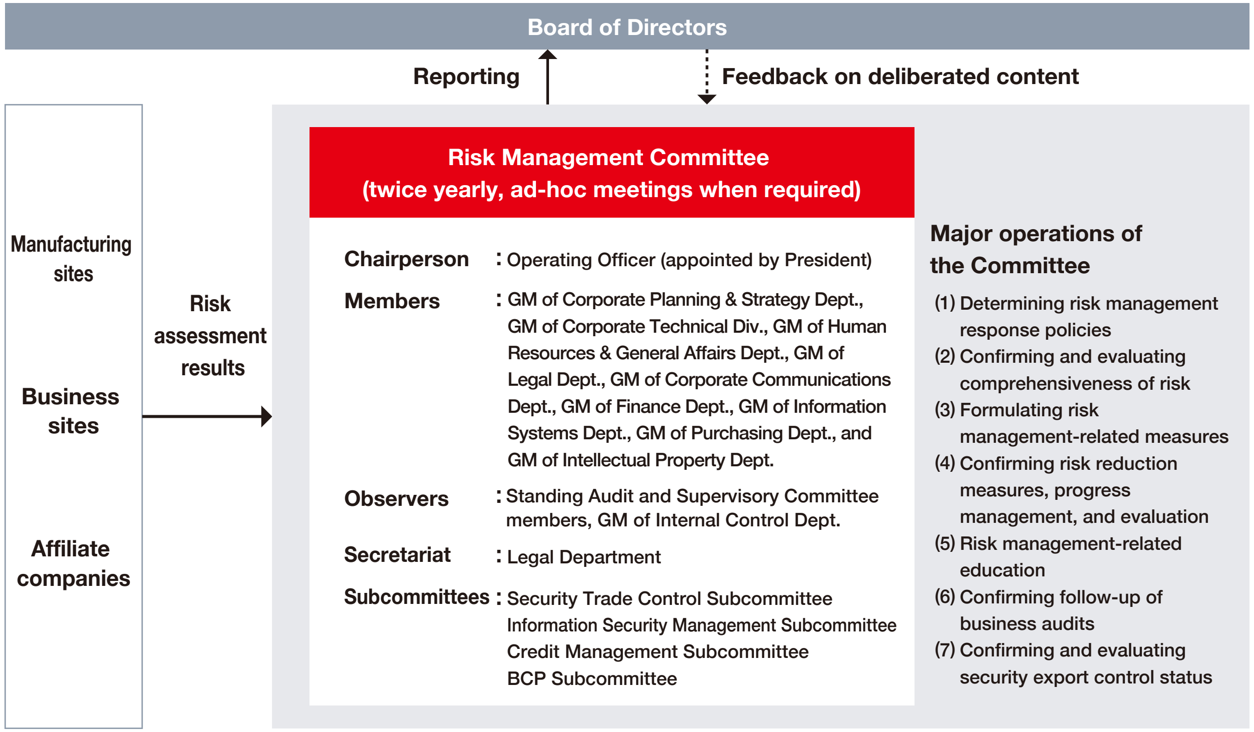
(3) We work to objectively verify the effectiveness of risk countermeasures by periodically conducting risk assessments, while working to recognize and evaluate new risks.

(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 Control 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.

Diagram of Risk Management Committee organization



Board of Directors

Reporting

Feedback on deliberated content

Manufacturing sites

Business sites

Affiliate companies

Risk assessment results

Risk Management Committee
(twice yearly, ad-hoc meetings when required)

Chairperson : Operating Officer (appointed by President)

Members : GM of Corporate Planning & Strategy Dept., GM of Corporate Technical Div., GM of Human Resources & General Affairs Dept., GM of Legal Dept., GM of Corporate Communications Dept., GM of Finance Dept., GM of Information Systems Dept., GM of Purchasing Dept., and GM of Intellectual Property Dept.

Observers : Standing Audit and Supervisory Committee members, GM of Internal Control Dept.

Secretariat : Legal Department

Subcommittees : Security Trade Control Subcommittee
Information Security Management Subcommittee
Credit Management Subcommittee
BCP Subcommittee

Major operations of the Committee

(1) Determining risk management response policies
(2) Confirming and evaluating comprehensiveness of risk
(3) Formulating risk management-related measures
(4) Confirming risk reduction measures, progress management, and evaluation
(5) Risk management-related education
(6) Confirming follow-up of business audits
(7) Confirming and evaluating security export control status

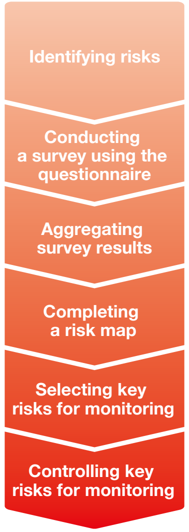
Corrective Process Against Negative Impacts | Risk Management

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

Risk assessment process

The Risk Management Committee takes the lead in preparing 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. Based on this list of risks, a questionnaire is sent to each NOF site and Group company to estimate the impact and frequency of each risk. Using the results of this questionnaire, the general managers of each division carry out risk evaluations. Based on the results, the Risk Management Committee identifies the risks whose response status should be recognized by management and consults with the Board of Directors to select the key risks for monitoring.

Flow of risk assessment

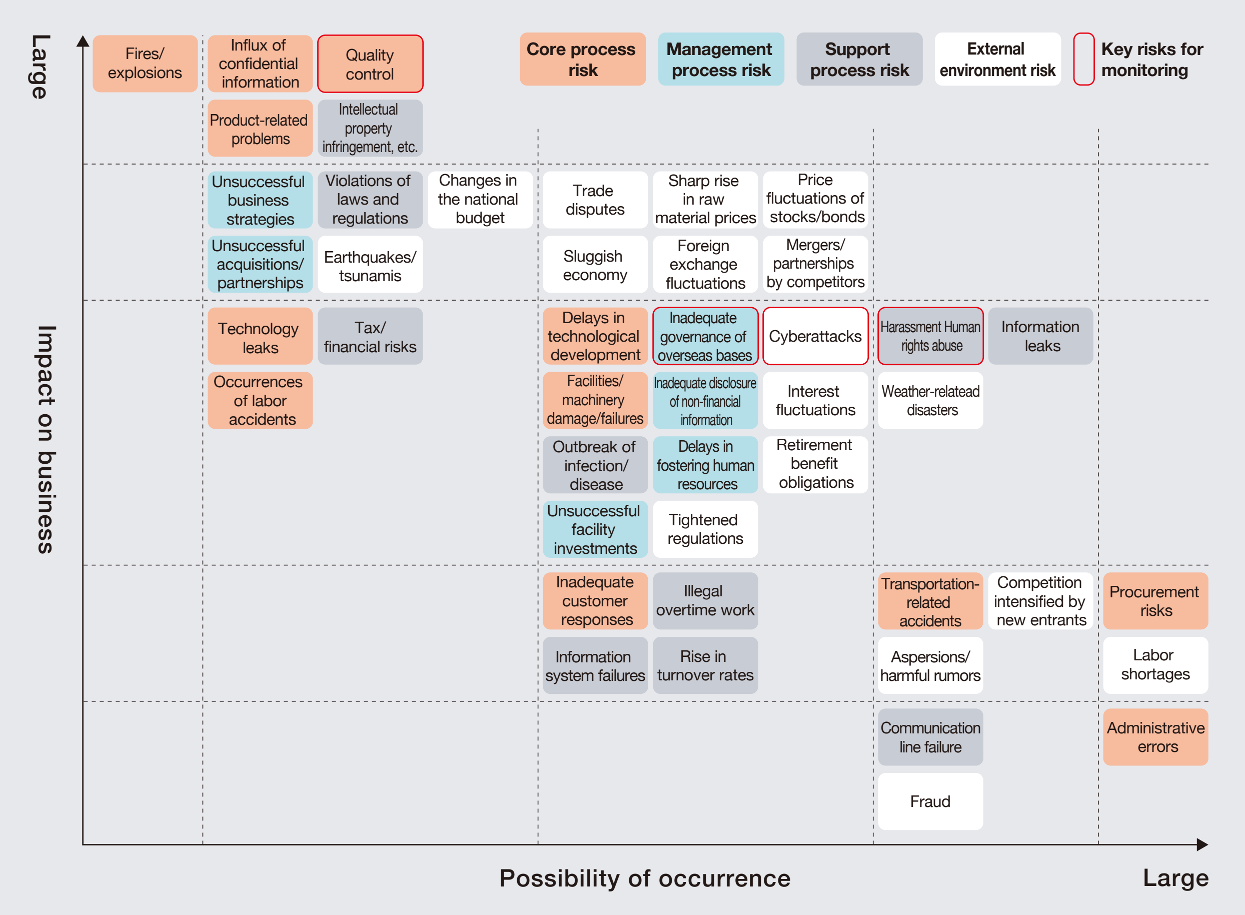


Identifying risks
Conducting a survey using the questionnaire
Aggregating survey results
Completing a risk map
Selecting key risks for monitoring
Controlling key risks for monitoring

- Identify expected risks of the NOF Group and prepare a list of risks
- With regard to the list of risks, managers of each department conduct a risk evaluation based on the questionnaire
- Aggregate the survey results and evaluate the impact and frequency of occurrence of risks to the NOF Group
- Prepare a risk map for the entire NOF Group based on the evaluation of the impact and frequency of occurrence of each risk
- Identify significant management risks from the risk list and risk map The Board of Directors selects key risks for monitoring
- The respective responsible committees report the progress of measures addressing key risks for monitoring to the Board of Directors

Risk map (excerpt)

The risk map is prepared based on the results of a questionnaire estimating the impact and frequency of risks at each NOF site and Group company, as well as the results of risk evaluation by managers of each department. The risk map is regularly revised and key risks for monitoring are selected in order to implement activities aimed at enhancing the NOF Group’ s resilience.



Core process risk
Management process risk
Support process risk
External environment risk
Key risks for monitoring
Large
Impact on business
Possibility of occurrence
Large
Fires/ explosions
Influx of confidential information
Quality control
Product-related problems
Intellectual property infringement, etc.
Unsuccessful business strategies
Violations of laws and regulations
Changes in the national budget
Trade disputes
Sharp rise in raw material prices
Price fluctuations of stocks/bonds
Unsuccessful acquisitions/ partnerships
Earthquakes/ tsunamis
Sluggish economy
Foreign exchange fluctuations
Mergers/ partnerships by competitors
Technology leaks
Tax/ financial risks
Delays in technological development
Inadequate governance of overseas bases
Cyberattacks
Harassment Human rights abuse
Information leaks
Occurrences of labor accidents
Facilities/ machinery damage/failures
Inadequate disclosure of non-financial information
Interest fluctuations
Weather-relatead disasters
Outbreak of infection/ disease
Delays in fostering human resources
Retirement benefit obligations
Unsuccessful facility investments
Tightened regulations
Inadequate customer responses
Illegal overtime work
Transportation-related accidents
Competition intensified by new entrants
Procurement risks
Information system failures
Rise in turnover rates
Aspersions/ harmful rumors
Labor shortages
Communication line failure
Administrative errors
Fraud

Corrective Process Against Negative Impacts | Risk Management

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

Overview and status of countermeasures of key risks for monitoring

Key risks for monitoring	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	● Revise the NOF Group Corporate Code of Ethics and the Compliance Manual ● Establish a consultation service with male and female employees as well as a contact point with attorneys ● Implement a company-wide employee engagement survey and feed back results to employees
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	● 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 appropriate, rational levels ● Raise the overall level of security measures at each company and promote stronger incident response capabilities
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 ● Strengthen communication through regular meetings with the NOF Head Office
Quality control	Possible decline in trust in the Company due to quality fraud, falsification of quality inspection results, and other situationsRisk of a significant increase in workload due to rising customer quality demands	● Ensure strict management of data related to quality control ● Raise awareness and train employees ● Conduct regular management audits

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 technology and technical information, which allows similar products/technologies to be 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
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 Law, 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 lecture and contact points for whistleblowing/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) ● Implement flood countermeasures for critical facilities ● Conduct BCP training and internal audits
Delays in fostering human resources	Possible stall in development of core human resources who will be responsible for business growth, due to a delay in implementing the human resource development plan	● 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
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	● Preparation of a roadmap for statutory disclosure ● Introduction of a system to optimize the collection and aggregation of sustainability information

Information security management

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

NOF considers information assets such as trade secrets and personal information entrusted to us by customers or business partners, or held by us, as well as systems for utilizing such information as important management resources in corporate activities. Based on the recognition that establishing robust information security for the information assets is essential for stable management, 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, we have established and published the Privacy Policy.

Under such policies, we have set forth specific measures for enhancing the levels of confidentiality, completeness, and availability of information and specific ways of handling personal information in our internal rules and manuals and are 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, Confidential Information Handling Manual, and Information Equipment Handling Manual.

(2) Management structure

In the internal organizational aspect, the Information Security Management Subcommittee is set up to deliberate and make decisions on important matters related to information security. Under the Information Security Management Supervisor, who is the chairperson of the Subcommittee, document information security management supervisors, electronic information and information system security management supervisors, personal information complaints handling supervisors, as well as a person responsible for management at each division, site, and department are appointed to manage the implementation of specific measures. Against threats such as unauthorized access from outside, information leakage, falsification, 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 such as trade secrets and personal information entrusted to us by customers or business partners, or held by the Group, as well as systems, etc. for utilizing such information (below, “information assets”) as important management resources in corporate activities. Based on the recognition that establishing robust information security for information assets is essential for stable management, we have established the below Policy and ensure compliance therewith.

(1) The NOF Group shall develop the information security system to further strengthen the management function of information assets.

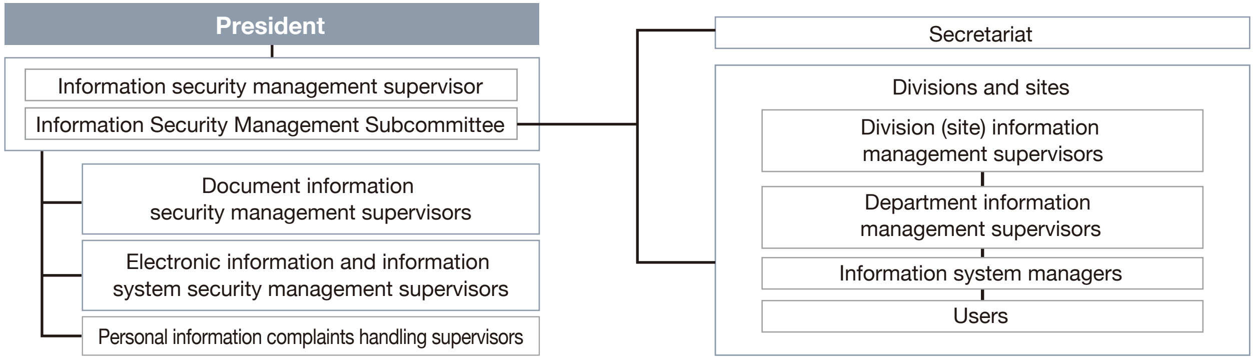
(2) In order to protect the information assets from leakage, falsification, and destruction, the NOF Group shall provide information security education for employees, develop regulations, and implement technical measures for information systems.

(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.

Diagram of NOF's information security management system



President

Information security management supervisor

Information Security Management Subcommittee

Document information security management supervisors

Electronic information and information system security management supervisors

Personal information complaints handling supervisors

Secretariat

Divisions and sites

Division (site) information management supervisors

Department information management supervisors

Information system managers

Users

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 reduction in technological competitiveness due to leakage of confidential or personal information	● Conduct self-inspections, and develop and implement improvement plans ● Information sharing through meetings of IT managers at domestic Group companies (once a year) ● Conduct training on handling suspicious emails (once a year) ● Respond by HDD encryption for computers taken outside the company and restrictions on the use of private storage media ● Provide information security-related e-learning training for employees (once a year)
Opportunities	● Improvement of corporate 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 primarily focus on the formulation of a manual to determine 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 plants and various government, infrastructure, and supply chain-related information required for resuming operations. Additionally, the BCP Task Force performs annual internal audits and training in an effort to firmly establish the BCP and enhance its effectiveness.

In fiscal 2024, based on the results of training from the previous fiscal year, we conducted company-wide joint training on the assumption of complex risks, including cyberattacks on overseas bases and the evacuation of Japanese employees from other countries. The training focused on smooth information sharing and cooperation between the Emergency Headquarters at the Head Office and local bases to verify the effectiveness of the BCP.

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