

Risk Management

Philosophy

JSR Group believes that preventing major crises from occurring and minimizing their impacts on business activities is a key part of management. In response to these issues, the Group has formulated Risk Management Policies and established a Risk Management Committee through which it actively pursues risk management activities.

Risk Management System

JSR Group has established a Risk Management Committee under the Sustainability Promotion Committee. We have put into place a system whereby the Risk Management Committee comprehensively manages important risks that have materialized or could potentially materialize within the Group.

The Risk Management Committee advances the Group's risk management by taking the lead in identifying important risks and supporting the formulation of policies for responding to such risks and the planning and execution of risk management plans by related committees or departments in charge.

For important risks that were identified, the progress of countermeasures is reported to the Sustainability Promotion Committee and the Board of Directors.

We manage risks related to the individual capital investments of each business, strategic investments such as M&A, and business plans through deliberations and decisions made by the Board of Directors and other committees.

The risk management system forms part of the Group's internal control system. The status of the internal control system's execution is reported regularly to the Board of Directors. JSR's Corporate Audit Department continuously verifies and evaluates the preservation and operation of internal control for the entire JSR Group as required by the Companies Act and Financial Instruments and Exchange Act. It also ensures that risk in existing business does not exceed permissible levels. Furthermore, the department additionally strives to maintain and strengthen internal control levels for the entire Group and conducts internal audits to ensure the appropriate and efficient execution of operations.



For details of our risk management structure, see our **Corporate Governance Report**.

https://www.jsr.co.jp/jsr_e/company/assets/pdf/20230704_CG_En.pdf

Identifying Risks and Selecting Important Risks

Under the initiative of the Risk Management Committee, each division of JSR Group companies in and outside of Japan identifies risks on a regular basis. In addition, management holistically understands risks related to management strategy and the foundation of business continuity.

Utilizing a risk map that represents level of business impact and frequency of occurrence, we identify risks that could have a significant impact on business continuity and organize them into JSR Group Risk Factors. We build and maintain a system for prevention of latent risks and crisis preparedness by having senior management monitor and regularly review important risks.



Please refer to the **JSR Sustainability Site** for more details.

https://www.jsr.co.jp/jsr_e/sustainability/governance/riskmanagement.shtml

Information Security Measures

JSR Group endeavors to manage information in an appropriate and secure manner by establishing Information Security Policy and by thoroughly disseminating the policy to its employees. Having established an Information Security Policy, JSR Group is working on the appropriate management of information by making this policy known to all employees. In August 2019, we established the Cybersecurity Management Office as the department in charge. We are working alongside outside experts on information security management including Group companies, employee training and education, and strengthening our response capabilities to cyberattacks or other incidents.

In FY2014, we published the Information Security Handbook so as to further increase employee sensitivity toward information leakage risks and to ensure their actions are in compliance with company rules at all times. We make employees aware of this handbook through our company intranet, e-learning, and workplace discussions.

In FY2022, using a ransomware attack as a scenario, we conducted a cyberattack response drill targeting members of HQ response team, including the President.

Crisis Management

JSR has formulated BCM procedures that summarize the BCM/BCP systems in place for both peacetime and emergency situations. In addition to defining the BCM organization and the actual BCP, which includes stipulations on target recovery times, and BCP activation and cancellation standards, these procedures also set out the organizational structure that takes effect during activations of the BCP, and corresponding priority businesses and operations.