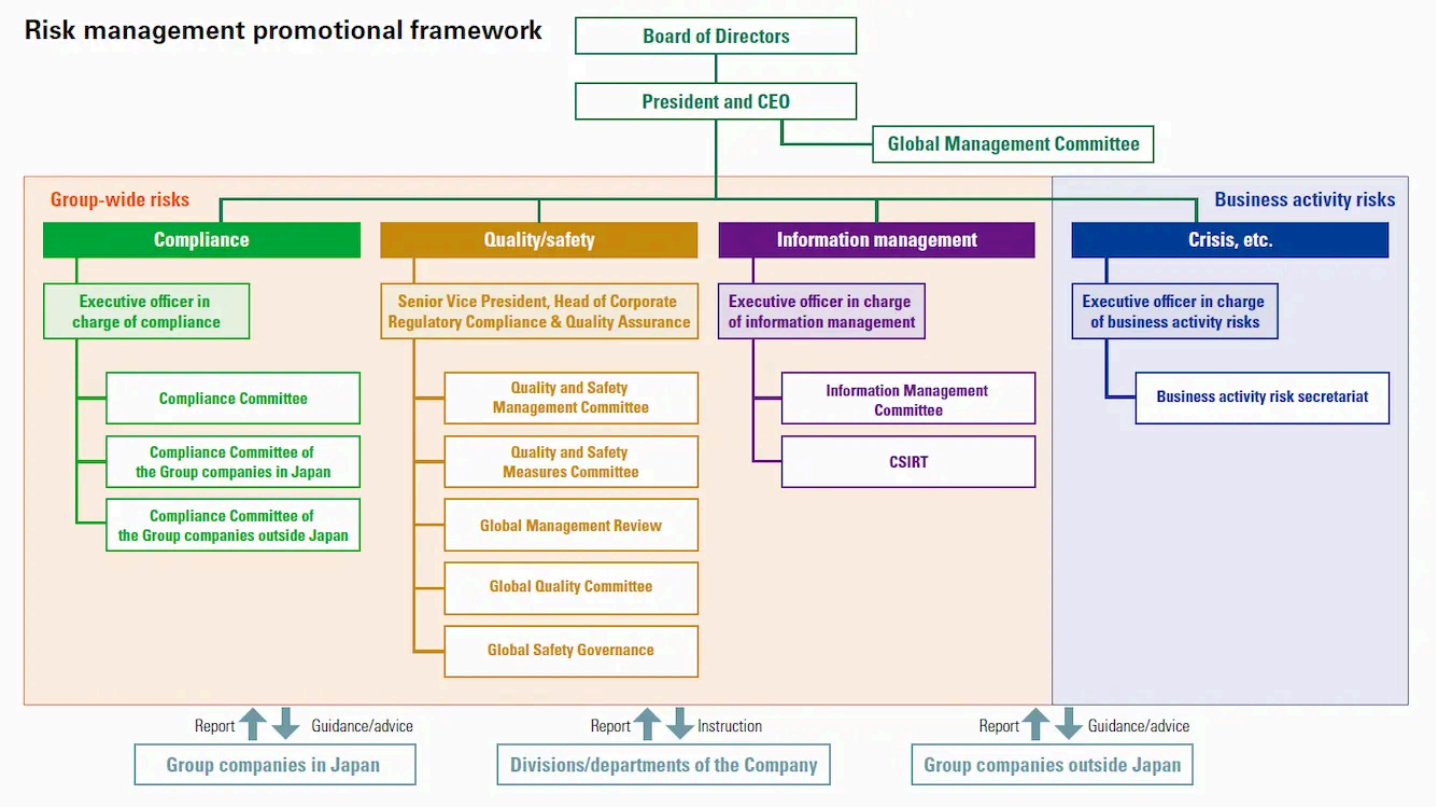
Sumitomo Pharma
Innovation today, healthier tomorrows

Risk Management | FY2023 Archive

Risk Management

Sumitomo Pharma has established the SMP Group Risk Management Policy that provides for basic thoughts of the Group with respect to risk management and has developed a system to appropriately promote risk management for the Group. Under this promotional framework, according to the particularities of each risk, risks are divided into those requiring a horizontal, group-wide approach (group-wide risks), and those requiring specific approaches by each company (business activity risks). The Company keeps track of the risk management of the group companies as a whole through reports from each group company, and provides each group company with its advice and guidance as necessary.

In order to address risks bearing an impact on business activities, we have established the internal "Risk Management Rule" under which it is clarified that the President and CEO's role in overseeing risk management, and developed systems to promote risk management for respective risks classified according to their characteristics. The status of operations in each system to promote risk management is periodically reported to the Board of Directors.
One of the Company's specific initiatives is to carry out annual risk assessments for all business units, including Group companies in Japan and overseas, and formulate necessary countermeasures based on the results followed by implementation and evaluation. This is undertaken systematically by each business unit company-wide working on the solution to each problem.



Rebuilding Business Continuity Plan (BCP) and Business Continuity Management (BCM)

From the viewpoint of our social duty of ensuring a stable supply of pharmaceutical products, Sumitomo Pharma formulates its business continuity plans (all-hazards BCP) that address not only large-scale disasters and pandemics, but also diverse disasters and unexpected situations. Furthermore, to strengthen and improve the effectiveness of our risk management, we have established a continuous management cycle that includes reviewing our BCPs, implementing proactive measures, and conducting education and training. Also, we are advancing sustainable business continuity management (BCM), which promotes management activities even during ordinary times.

Initial Response Plan

We have established a Crisis Management Team (CMT)* that, immediately after a disaster occurs, starts gathering information, outlines the status of damage, offers advice on whether a Disaster Management Headquarters should be established, and if established, works to gather further information. We carry out regular CMT training and other measures with the objective of increasing our swift and precise first-response capabilities. We are currently carrying out training to facilitate coordination between the CMT and administrative offices (the Disaster Management Headquarters in the disaster area) as well as the Disaster Management Headquarters, and are working to boost crisis management capabilities during times of disaster.

* CMT (Crisis Management Team): A team that is quickly assembled after a disaster breaks out, then starts gathering information, surveying the status of damage, and offering advice on whether a Disaster Response Headquarters should be

established. If a Disaster Response Headquarters is established, the CMT continues gathering information, outlining the situation, and conducting similar tasks.

Information Management

"Information" is an essential asset in our corporate activities, and how it is utilized and protected is of particular importance to Sumitomo Pharma. We have established global policies for records and information management as well as various rules for information management and Information Technology security, etc. to minimize risks.

Management of Confidential Information and Inside information

In accordance with the internal rules, we manage confidential information in an appropriate manner. We have established an information management system that includes an executive officer in charge of information management and the Information Management Committee. In order to prevent insider trading, we have internal rules which specify matters that all officers and employees must comply with, including the appropriate management of inside information. Additionally, we regularly hold training for officers and employees and we work to increase their level of awareness.

Managing Personal Information

Sumitomo Pharma has a privacy policy in place, and in accordance with its internal rules, properly handles and protects personal information acquired through its business activities from healthcare professionals, product users, business partners, shareholders, officers and employees and other persons in accordance with domestic and international personal information protection laws and regulations. In addition, Sumitomo Pharma actively promotes protection of personal information by establishing a solid management system that includes an executive officer in charge of personal

information management and a personal information hotline, and regularly educating and training its officers and employees.

Information Security

As information security efforts, we continue to update technical measures, internal rules, and procedures according to societal changes and advances in information technology as we monitor compliance. In addition, we hold periodic information security training for officers and employees to raise awareness. We also strive to address information security risks at our group companies and business partners. Further, as a countermeasure against information security risks throughout the supply chain, we conduct IT security assessments of our business partners using a security rating service. Moreover, we consider preventive measures against unauthorized access due to cyberattacks and have established a system that responds rapidly in the event of detecting an intrusion, through a Computer Security Incident Response Team (CSIRT). We also continuously work to prevent information security incidents. CSIRT also conducts regularly response training that presents a cyberattack scenario.