promotional activities of MRs and others, and with regard to the behaviors that could have been taken as a violation of the Guidelines, the information was shared with the parties concerned as well as the relevant promotion department to raise awareness and prevent violations. In addition, we continuously remind MRs and others of the importance of compliance with the Guidelines and other industry-related norms during training sessions.

As a life-related company, we will continue to work to further improve our ethics, transparency, and credibility while conducting activities to deepen the understanding of medical institutions and medical professionals.

Code of Practice

As a responsible life-related company that handles pharmaceuticals, ASKA Pharmaceutical recognizes the need to ensure a high level of ethics and transparency in its corporate activities. Based on this recognition, in FY2013 we established the ASKA Pharmaceutical Code of Practice as a code of conduct for all Board members and employees and their interactions with researchers, medical professionals, patient groups, etc., and we are implementing corporate activities that can be understood by society by ensuring that all Board members and employees are fully aware of the code.

Risk Management

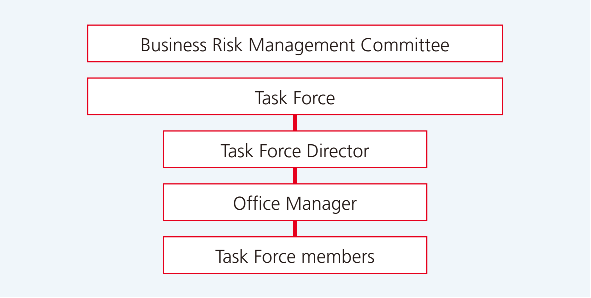
Basic Policy on Risk Management

In order to deal with risks that may affect the business activities of the Group, we have established the Group Business Risk Management Rules and are implementing a risk management system with classifications based on characteristics and risks. Each department prepares and operates procedure manuals and systematically works to resolve issues through annual risk assessments and the formulation, implementation, and evaluation of countermeasures based on the results of those assessments.

Risk Management System

Every organization within the Group has formulated and implemented a business risk management manual in a bid to avoid risks and minimize damage. If crises actually occur, the Task Force takes action as necessary.

- Group Business Risk Management System



Business Continuity Plan (BCP)

In order to ensure a stable supply of pharmaceuticals and other products, we have formulated three types of BCP: one for natural disasters such as large-scale earthquakes and tsunamis, one for the spread of infectious diseases such as the novel influenza, and one for security incidents. We are working to establish a system that will enable us to quickly restore our business activities. Going forward, we will continue to enhance our preparedness for anticipated risks, conduct employee awareness activities, and further improve our crisis management system.

Information Security

The Group recognizes that the appropriate management of information assets is an important management issue and has implemented the following measures to ensure safe and secure management.

1. Establishment of information security management system
   The Group has established an information security management system to protect information assets held by the Group and to maintain and improve information security.
2. Establishment of internal rules for information security
   The Group has established internal rules for information security in order to appropriately manage information assets.
3. Education on information security
   All Board members and employees of the Group are informed of the importance of information security and the proper use of information assets held by the Group.
4. Implementation of information security measures
   The Group takes appropriate countermeasures—measures to prevent and correct unauthorized access to, loss, leakage, falsification, and destruction of information assets.
5. Compliance with laws and regulations
   The Group shall comply with laws, regulations, and other relevant norms related to information security.
6. Maintenance of audit system
   The Group shall strive to ensure information security by establishing an internal audit system to check and evaluate the status of compliance with laws, regulations, and internal rules.

Cybersecurity

The Group works to prevent risks such as unauthorized access and data leaks before they occur and takes prompt corrective action in the event of an incident. We also address emerging threats such as ransomware and attacks using generative AI, maintaining 24-hour monitoring with the latest security tools. In OT security, which covers manufacturing facilities, and IoT systems, we have implemented network segmentation and multilayered defenses to ensure safety. In addition, we provide thorough training for Board members and employees, raising awareness through phishing simulations and the sharing of real-world cases.