Governance

Risk Management

Risk Management Structure

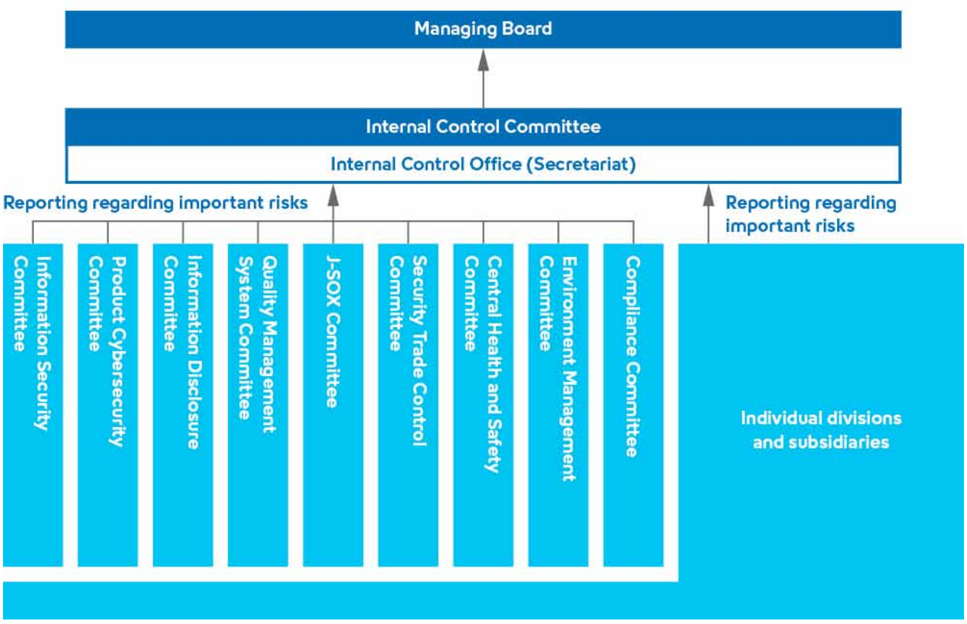
Risk Management Structure

Promoting Risk Management by Establishing a Dedicated Committee

Sysmex established the Internal Control Committee to supervise risk management of the Group as a whole, and promotes all risk management activities, including those regarding strategic risks. The Committee is chaired by the President and its members include relevant executive officers and Audit and Supervisory Committee members (excluding outside members of the Managing Board, who act as observers).

By regularly assessing risks involved in such areas as fair trade, compliance (including corruption and business ethics), human resources, occupational health and safety, the environment, and accounting and finance (including tax payments), the Committee identifies risks significantly affecting the Group’s operations and takes necessary countermeasures. In addition, it monitors the status of risk management by relevant committees, including the Compliance Committee, as well as individual divisions and subsidiaries, and periodically reports to the Managing Board. When a major risk that has a significant impact on the Group’s business arises, the Internal Control Committee also reports to the Managing Board to discuss how to respond, following the PDCA cycle.

Risk Management Structure


Managing Board
Internal Control Committee
Internal Control Office (Secretariat)
Reporting regarding important risks
Reporting regarding important risks
Information Security Committee
Product Cybersecurity Committee
Information Disclosure Committee
Quality Management System Committee
J-SOX Committee
Security Trade Control Committee
Central Health and Safety Committee
Environment Management Committee
Compliance Committee
Individual divisions and subsidiaries

▶ Corporate Governance

▶ Sysmex Report (Risk Management)

Governance

Response to Risks Related to Business Continuity

Establishment of a Business Continuity Plan (BCP)

Response to Major Disasters

Sysmex has formulated Group-wide business continuity plans (BCPs) for production, procurement, and other functions to ensure the continuity of important operations in the event of an earthquake, storm or flood damage, and other large-scale disasters, as well as rapid recovery from such disasters.

In addition, we relocated our distribution center to an inland location with less risk of flooding so we can reinforce our system for stable supply even further. We also strengthened the facility with a quake-absorbing structure, private power generation system, and fire shutters.

Main BCP Approaches:

- Decentralization of main raw material procurement (selection of production locations based on the concept of local production for local consumption)
- Establishment of a mechanism for procurement of parts such as semiconductors with long lead times to register raw material ordering plans for such parts in a system based on our medium-term production plan
- Decentralization of product storage according to storage function (instruments, maintenance parts, room temperature storage reagents, cold storage reagents, and hazardous reagents)
- Creating mutual supply systems within the factories, and securing alternative routes for transportation of products
- Prioritizing important products for supply to medical institutions
- Introduction of a tool (cloud system for disaster prevention information) to share crisis information between the Company and raw material suppliers so the Company can promptly take measures against highly urgent risks such as a natural disaster, fire, or accident occurring on the supplier side
- Providing rules and manuals for disaster response and conducting regular disaster drills
- Introduction of an employee safety confirmation system
- Installation of digital radios in each business office
- Provision of emergency supplies and items to support employees staying at business offices and returning home after a disaster
- Establishment of basic IT systems (assignment to an external data center and creation of a system infrastructure that is quickly transferable to a backup system in emergencies)

▶ Undertaking the Never-Ending Mission of “Creating a Stable Supply of Reagents”

Governance

Enhancing Information Security

Enhancing Product Security and Cyber Security

Product Security Initiatives

Sysmex Corporation has established a Product Security Policy for our products and services and has established a Product Security Incident Response Team (PSIRT) to manage product design and manufacturing, as well as post-marketing vulnerabilities. Sensitive information (including individual, patient, and test subject information) obtained from our customers, and those who have participated in research and development and experiments, as well as advanced, original technology regarding products and intellectual property, are considered important assets for management, and necessary measures are taken to prevent information leaks and internal fraud.

Information and Cyber Security Initiatives

We formulated the Information Security Policy to establish a Groupwide information security management framework. This creates an information security management system for the entire Group under the supervision and management of a Member of the Management Board, a senior executive officer,and a senior managing director, who acts as Information Security Officer, with the DX Strategy Development Division at its core. We established a Sysmex Computer Security Incident Response Team (Sysmex-CSIRT) to bolster our initiatives such as prevention and early response to incidents and pre- and post-response to information leaks and data breaches, based on such information as alerts received from the managed SOC (security operations center) and threat information (threat intelligence) received from external parties (JPCERT/CC).

Regarding collaboration with external organizations, we participate in the Medical Device Cyber Security Council, whose members include representatives from the Ministry of Health, Labour and Welfare, hospitals, and domestic medical device manufacturers. We have also joined the Nippon CSIRT Association and Forum of Incident Response and Security Teams (FIRST) to share information regarding threats from emergencies and other significant incidents.

Internally, we have implemented specific measures including rigorous management and regular review of access to information, regular updates to security patches, login restrictions by biometric authentication (facial and fingerprint recognition) for laptop computers and mobile devices on loan from the Company, and reviews of installed applications. In addition to these operational and control measures, we also installed endpoint detection and response (EDR) for PCs and server devices as part of our ransomware countermeasures.

Information and Cyber Security Education

At Sysmex, we provide annual e-learning on information security for all our Group employees, as well as temporary employees and independent contractors. In fiscal 2022, we held cyber security training in multiple languages for all employees in the Group. We are also implementing initiatives to raise employee awareness of information security, such as seminars concerning how emails should be handled, as well as drills for targeted email attacks (BEC and phishing).

We recommend that Sysmex-CSIRT members obtain international qualifications (ISC2 CISSP, SANS GIAC, CompTIA) to reinforce our response to security incidents.

Acquiring Information Security Certification

Sysmex Corporation has obtained ISO 27001 certification for our Information Security Management System (ISMS), and we are enhancing our information security management for research involving gene sequencing and other personal information. The service and support division of Sysmex CNA has obtained the same certification. Sysmex UK and Oxford Gene Technology have obtained Cyber Essentials※ certification as well as ISO 27001 certification, and undergo a surveillance review every six months.

※ Certification system initiated in 2014 by the UK government to improve corporate cyber security

▶ Information Security Policy
▶ Product Security Policy