Basic Approach and Governance

Information security is integrated into our business plan as a major risk, and the Board of Directors and Audit Committee oversee all critical corporate risks, including information security. The Board of Directors and executive officers administer enterprise risk management for the entire Group, and information security is one of the core areas. Risk management for each region and function is based on the instructions of the executive officers, and priority measures for information security in business plan are implemented by the heads of each business and function based on risk assessment. Among the executive officers, the CAO assumes executive responsibility in the area of information security, and the Chief Information Security Officer (CISO) strengthens the governance of business execution under CAO's delegation. The CAO reports regularly on the status of information security to the Group Executive Committee and the Board of Directors.

Promotion Structure

To ensure the appropriate management and protection of information security concerning the business, the information security management structure is formed under the CISO with clear responsibility assignments. Under the direction of the CISO, and under a global governance structure that incorporates four information security areas, we will work to manage and ensure information security.

Four areas of information security	Definition
Information security governance and strategy	Manage information security risks and formulate strategies.
Product security	Ensure security of products across their life cycles, including the supply chain.
Enterprise information security	Ensure enterprise information security, including cyber security, IT security, and physical security.
Data protection	Ensure management of property damage risks by incorporating risk control processes that are compliant with legal obligations, and which include appropriate data classification and specification of privacy requirements, within our business procedures.

Initiatives (Management)

Information Security Risk Management

The Olympus Group implements the PDCA (Plan-Do-Check-Act) cycle, which includes assessment, analysis, planning and implementation based on four areas of information security, and review of implementation results, according to the necessary hierarchy. In the assessment process, we incorporate information from multiple third-party perspectives, including domestic and overseas regulatory ministries and agencies, government agencies related to information security, independent agencies, industry organizations, and threat intelligence vendors, as well as strive to gain a global understanding of our own situation. In addition, in order to formulate effective countermeasures for the analyzed risks, we classify the risks appropriately and examine them from multiple perspectives, including our own initiatives, collaboration with relevant organizations, and risk assurance.

Risk Management Processes

The Olympus Group conducts third-party assessments, including a penetration test to evaluate vulnerabilities, as well as global monitoring of information security incidents, and takes measures to address risks according to any observed incidents.

Risk Mitigation

Incident Response: To respond to IT security incidents, we have clarified the global rules, and the global Information Security Governance Committee, which is formed under CISO, shares information on incidents as the situation demands. We conduct trainings in order to maintain the effectiveness of our incident response system. In light of the recent frequency of cyber attacks, the incident response plan is constantly updated as necessary to ensure global information security. Regarding product security, we have established a system to collect information on threats and vulnerabilities related to our products and analyze security risks, and are working to implement security measures as soon as possible. As for data protection, we are implementing appropriate protection by classifying the importance of data from the perspective of compliance and risk control, as well as related laws and regulations, and introducing appropriate management methods.

Business Continuity Plans: In order to minimize the impact on business operations in the event of an incident, we have identified the most important operations and information assets throughout the Company and in each function and division, and are developing emergency systems and procedures to maintain and protect them.

Information Security Education: Education through e-learning and other means, as well as awareness of the information security policy and incident reporting process, is being implemented in all regions.

Information Security

https://www.olympus-global.com/csr/governance/security/