## Risk Management

### Basic Approach

Changes in global circumstances, the globalization of business, and other factors are causing rapid changes in the Terumo Group’s business environment. At the same time, risks affecting our business activities are diversifying and growing in complexity. In response to these risks, the Terumo Group is moving forward with the construction of a Groupwide risk management system, an effort that began in fiscal 2015.

The Group Risk Management Policy provides the guidelines for appropriate risk management based on identification and analysis of risks for the Group as a whole. Our objective in managing risks is to provide the proper environment for supporting bold yet appropriate risk-taking—for all types of risks—by management and ultimately to win stakeholder faith and enhance our corporate value.

Messages are communicated to all associates from Terumo’s President and CEO stressing the importance of risk management as part of corporate activities. These messages are underscored by a target of realizing an organizational culture in which each individual associate is conscious of risk as they perform their job responsibilities.

### Risk Management System

#### Establishment of Risk Management System

The Risk Management Committee has been established directly under the Board of Directors as an organization charged with overseeing risk management across the entire Group. Chaired by the President and CEO, the committee’s membership includes officers at the level of Managing Executive Officer and higher, representatives of relevant departments selected by the committee chair, and the Company’s legal counsel. The committee meets twice a year to discuss key risks and draw up, implement, and monitor risk response measures.

Key risks are designated by assessing risks identified throughout the Group based on predefined criteria. Assessment criteria focus on two key points: 1) whether the risk will significantly impact patients and Terumo customers, and 2) whether the risk will cause serious damage to the Terumo Group’s management. Risk information is gathered from throughout the Group, organized in a database, and shared with department heads and risk managers at subsidiaries. In addition, a system has been established for information to be communicated to management organizations promptly through functional departments and the relevant departments of subsidiaries when a significant issue arises.
Risk Management

Risk Management Education
Since fiscal 2016, we have been including content emphasizing the importance of risk management in briefings for department heads and conducting participatory workshop training for associates. Through such initiatives, we are working to enhance the level of risk sensitivity among individual managers and associates.

Crisis Response
When a crisis emerges (an identified risk occurs), the Group Risk Management Policy stipulates that an internal response be organized in accordance with the crisis level. Crisis responses aim to accomplish three things: 1) protect human lives, 2) minimize damage and losses, and 3) maintain the trust of society. Should a crisis of the highest level occur, we will establish a crisis response headquarters, led by the Risk Management Committee Chair, with the relevant department heads as the second tier of leadership.

Responses to Major Disasters and Other Emergencies
The Terumo Group provides medical devices, pharmaceuticals, and services that are directly linked to people’s lives. Accordingly, we believe that ensuring business continuity in the event of a major natural disaster or some other unforeseen situation is an important social obligation of the Group.

We have therefore prepared business continuity plans (BCPs) to prevent our operations from being disrupted even under extreme circumstances and to ensure that operations can be quickly restored and resumed should they be disrupted. We conduct various drills on a regular basis and implement other countermeasures.

If a large-scale disaster strikes, a disaster response headquarters, led by the President and CEO of Terumo Corporation, will be established to swiftly initiate response activities. The disaster response headquarters will ascertain the condition of associates and their families, and gather information on matters such as conditions of suppliers and in disaster-hit areas to assess the current situation, so that response actions can be determined and implemented. At the same time, the disaster response headquarters will embark on efforts to provide the necessary support to disaster-hit areas in a timely manner.

If it becomes apparent that the Terumo Group’s supply chain or operations will be temporarily interrupted, the disaster response headquarters will transition to a business recovery mode and begin work to restore normal supply chain and operational functions as quickly as possible.

Business Recovery Organization

---

[Diagram of Business Recovery Organization]

---

SUSTAINABILITY DATA BOOK 2020
59
Business Continuity Plans
Based on the Group BCP Policy, the Terumo Group has developed BCPs for its operations around the world based on three policies: 1) fulfill our social responsibility. That impacts to the healthcare system should be minimized whenever possible, 2) protect our associates and their families worldwide, and 3) protect our assets. BCPs have been prepared for factories, functional departments engaged in tasks such as raw material procurement and distribution, and Companies. By promoting disaster preparedness in all divisions, we aim to ensure swift and accurate responses in cases of emergencies.

Preparedness Drills
Each Terumo Group location conducts drills, such as the following, on how to respond to large-scale natural disasters. Communication drills are also conducted jointly with Terumo's logistics partners.

- Establishment of a disaster response headquarters following a major earthquake, confirmation of the roles of individual staff, and other BCP-related drills
- Implementation of systems for rapidly ascertaining the condition of associates and their families and training on their use
- Comprehensive disaster response drills including firefighting, CPR, and rapid evacuation

Infectious Disease Countermeasures
Terumo has been designated as a specified public institution under Japan’s Act on Special Measures for Pandemic Influenza and New Infectious Disease Preparedness and Response. Accordingly, we have developed an operation plan as required and have formulated a BCP that will enable us to continue operating even in the event of an outbreak of a new strain of influenza or other infectious diseases.

In addition, Terumo has prepared its infectious disease response manual to guide efforts to combat the various infectious diseases that are currently spreading around the world and to help halt the spread of such diseases. This manual lays out rules covering everything from infection prevention to the return to work of associates who have been infected in an effort to protect business operations from the impacts of infectious diseases. Terumo also monitors the status of infectious diseases around the world and issues travel precautions or restricts business travel for its associates, as conditions warrant.

Information Security
Basic Approach
In pursuing business operations, we, at the Terumo Group, take measures to properly protect and ensure information safety with regard to confidential information of the Group as well as information entrusted to the Group by customers and business partners from all manner of threats, including unauthorized access by outside parties; information leaks due to negligence; information manipulation, destruction, and theft; information system malfunctions; and natural disasters. The Group Information Security Policy has been established as a shared global policy for information security, and region-specific information security rules have been formulated based on this policy. Regarding personal information, we have developed the Personal Information Protection Standard based on Japanese laws and regulations, including the Act on the Protection of Personal Information and Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures. We properly protect and manage all forms of personal information, including Individual Number (used for Japan’s Social Security and Tax Number System), in accordance with these standards. Furthermore, we have established procedures to be globally compliant with the General Data Protection Regulation, a new personal information protection regulation implemented by the European Union in May 2018.
Information Security System

Under the direction of the Chief Information Officer (CIO), the Terumo Group develops global information security systems headed by the IT Planning Department. The formulation and enactment of standards and guidelines based on the laws and regulations of countries of operation and the education and training of associates are promoted on a global basis through these systems. In addition, global meetings are held regularly between representatives from Terumo’s IT Planning Department and information security divisions of Group companies. These meetings serve as opportunities to share information on cyber risks and other matters and to examine possible measures for strengthening information security.

In Japan, information security managers and management staff are appointed in each department of Terumo and in each Group company, as stipulated by the Group Information Security Policy and the information security rules. These individuals perform management and provide guidance to ensure that information in their departments is properly managed and protected. Outside of Japan, information security officers are selected for each region and information security managers are put in place at all affiliates to promote appropriate information protection and management throughout the Group.

Global Information Security Management Organization

Measures for Strengthening Information Security

Terumo business locations throughout the world perform self-evaluations of their security status annually, and information security training for associates is conducted on a regional basis once a year. In addition, both internal and external audits are performed to confirm the status of compliance with the internal rules and regulations of the Company.

We have recently seen a rise in the various information security threats needing to be addressed, including targeted attacks, unauthorized access, and leaks of personal information. To combat such threats, we are implementing measures for strengthening information security to provide multilayered protection that includes countermeasures for scam emails, monitoring for unauthorized transmissions, and other provisions. Furthermore, we conduct drills on targeted email attacks for our associates around the world to raise their awareness of information security.