Business Risks

The most common risks that could potentially impact the Group's business performance results and financial condition are outlined below. While these are the most common risks, they do not represent all potential risks.

The items covered herein are possible future occurrences determined by the OTSUKA Group as of March 27, 2020.

Customer-related Risks

The OTSUKA Group's customers range from large enterprises to small firms that span a broad range in terms of company scale and industries. Consequently, its level of dependency on any specific customer is low.

However, the Group's operations could be impacted by convergent changes in IT investment trends by a large number of companies as a result of unexpected changes in the economic environment.

Supplier-related Risks

The OTSUKA Group is supplied with high-quality products, services and technologies (hereafter called "products") by numerous suppliers for respective segments in order to optimally resolve the problems of each customer. While working to deepen its relationship with suppliers to ensure stable supply of these "products," the Group is constantly working to acquire information on newer "products" as well.

However, the Group's operations could be impacted by the inability to supply "products" in the quantity demanded by customers because of insufficient supply of "products" due to issues at supplier sites, as well as by the Group's inability to obtain substitutes.

Information Leakage Risks

The OTSUKA Group possesses an abundance of individual and corporate information pertaining to operations that is handled carefully. The Company received approval to use the Privacy Mark of the Japan Institute for Promotion of Digital Economy and Community, and its Internet Data Center acquired certification for Information Security Management Systems (ISMS).

As a concrete measure to manage data, the Company has released an internal and external Personal Information Protection Policy, as well as established regulations on personal information protection, confidentiality and information system security. The Company has its employees take a pledge of confidentiality as well as works to prevent information leakage outside of the Company and raises awareness of information management through its proprietary educational "CP (Compliance Program) License System" and other measures. Moreover, the Company implements even more stringent measures for its information systems. These include respective technical measures used at entrances, internally, and at exits as well as third-party external diagnoses, regular drills against targeted e-mail attacks and establishing the Computer Security Incident Response Team (CSIRT) and the Security Surveillance Committee.

Even with these measures, however, the Group's operations could be impacted by assuming liabilities for damage and loss of trust by society in the unlikely event that personal or corporate information is leaked outside the Group.