RISK MANAGEMENT

Risk Management Policy

The Group conducts an annual review of risks that may affect the achievement of the new medium-term management plan and existing business, and maintains a "management crisis list." This list sets out risks with the potential to have a significant impact, which are classified as "material risks." These include risks that require rapid contingency measures in addition to normal controls and for which risk avoidance, reduction, transfer, and other measures should be initiated with a priority classified as "significant material risks." For each "material risk," the Group as a whole promotes focused control activities, and for "significant material risks," it implements a risk management cycle (PDCA) by regularly monitoring the status, confirming the effectiveness of response, and making recommendations for improvement. We are also engaged in other activities necessary for the uptake and thorough implementation of risk management.

The following is a list of 11 items that could have a significant impact on the achievement of the Group's business plan and on the Group's existence. One of these risks has been designated as a "notably significant risk" and is being addressed as a priority.

Notably Significant Risks

	Risk items	Countermeasures
1. Risk of cyber-attacks	Some cloud services offered by the Group include services involving the handling of important customer data, such as institutional accounting, management accounting, and business management. In the event of a service outage or loss of customer data due to cyber-attacks on those services, there could be a significant impact on customer operations. In addition, we recognize that this is a significant important risk because the occurrence of such an event for reasons attributable to our Company could have a material impact on our Group's performance and financial position, including the payment of compensation for damages, and could also lead to a decline in the credibility and brand image of our Group. We recognize that this is a particularly important risk.	The Group has established a security organization to reduce risk, and is continuing risk identification and improvement activities to promote system failure countermeasures such as multiple data backups and other security measures such as multi-factor authentication. In addition, we have obtained SOC1 Type2 reports for some of our cloud services in compliance with the U.S. Statement on Standards for Assurance Engagements No. 18 (SSAE18), and we strive to improve the quality of system operations by utilizing objective evaluations from a third-party perspective. During the period under review, we focused on the "recovery" aspect of the cyber security framework, and are working to develop a mechanism for data preservation and rapid recovery.

Next, we will go through risks that we recognize as very important, but that will not have a significant impact if they materialize, or risks we believe we can adequately address before they materialize.

Significant Risks

	Risk items	Countermeasures
2. Risks related to equity investment and M&A	The Group aims to achieve sustainable earnings growth and business expansion under its new medium-term management plan, BE GLOBAL 2028. To this end, the Company's policy is to make acquisitions and enter into capital tie-ups as necessary, while taking into account its performance and financial position. However, in proceeding with M&A, there is a possibility that the transaction will not proceed as envisioned by our Group due to an inability to find suitable candidates or to reach agreement on transaction terms, etc. In addition, problems that cannot be identified in preliminary investigations, such as the occurrence of contingent liabilities or unrecognized liabilities after the investment or M&A, may lead to impairment of goodwill, etc., which may affect our Group's performance and financial position. In addition, problems that cannot be identified in the preliminary investigation, such as the occurrence of contingent liabilities or the discovery of unrecognized liabilities after investment or M&A, may lead to impairment of goodwill or other losses, which may affect the Group's performance and financial position.	The M&A organization conducts detailed due diligence on the financial position and contractual relationships of candidate companies in advance, and makes decisions based on the verification of each identified risk and countermeasures. We also strive to reduce such risks by quantitatively and qualitatively understanding the business conditions of the investee companies involved in each business.
3. Risks related to business investment and capital expenditure	In order to achieve the goals of the new medium-term management plan, the Group is investing in human resources and R&D, as well as in product development to strengthen product competitiveness, and in the development and expansion of its business infrastructure. However, it is possible that these business investments may not produce the expected investment results due to changes in the market environment or a gap between developed products and market needs. If the investment does not produce the expected effect, the Group's performance and financial position may be affected in the medium to long term.	In response to this risk, the Group carefully decides on business investments at the consideration stage after evaluating investment effects and risks in accordance with the authority stipulated in the "Authority Regulations" in advance. We strive to prevent risks from materializing and reduce their impact.
4. Risks related to securing and fostering human resources	If the Group's ability to secure and develop talented human resources with the expertise needed to promote its business and achieve growth does not proceed as planned over the medium term, the Group's future growth potential and business performance and financial position may be affected.	In addition to strengthening our recruiting system and ensuring competitiveness in recruiting by understanding the market's appropriate remuneration levels, we are also promoting measures to enable new employees to contribute to the Company as soon as possible, such as by enhancing our training menu for new hires.
5. Risks related to dependence on management	Although our Group's organization is currently working to develop human resources and establish an organizational structure, we recognize that our management is highly dependent on Tetsuji Morikawa, our President and Representative Director, and if something unexpected were to happen to the President and Representative Director, it could affect the promotion of our business activities and our business performance and financial position.	To address this risk, we are working to formulate and execute a succession plan by appointing the next generation of leaders as directors of operating companies and entrusting them with the management of these companies, and by providing supervision and guidance from the holding company to develop successors.
6. Risks related to system outage of cloud service data	If a failure occurs in the cloud services provided by our Group and the operation of the system or service is suspended, it may have a significant impact on customer operations. In addition, if problems such as loss of customer data were to occur, the impact would be even greater, and in some cases, compensation payments for damages incurred could have a significant impact on our Group's performance and financial position. In addition, any delay in the operation of the service will lead to a deterioration of the Group's social credibility and brand image.	To address this risk, we are promoting various measures to prevent failure and minimize the impact of failure so that our systems can operate stably and services can be provided continuously.

	Risk items	Countermeasures
7. Risk of legal violations	The Group believes that an effective compliance system is essential to fulfilling its social responsibilities as a corporation.	To ensure that the compliance system functions effectively in response to this risk, the Group formulates compliance rules and other compliance-related regulations, and ensures that all officers and employees are fully aware of them through education and training. In addition, the Compliance Committee promotes compliance activities by establishing quantitative checkpoints for compliance.
8. Risks related to service quality	The Group provides support for the introduction of software developed in-house or by third parties that is systematized according to customer needs, contracted development, and BPO services for undertaking financial closing operations. In the provision of services, there is a possibility that deviations from initial estimates may occur due to ambiguities in contractual content or requirements, or that unforeseen technical problems or project management issues may arise, resulting in increased costs and delays in schedules. If such a problem were to occur, the Group's performance and financial position could be significantly affected due to higher-than-expected costs and compensation payments for damages resulting from delays in delivery.	To address this risk, we are taking measures to reduce the impact on our business performance and financial position by purchasing insurance to cover contingencies, while improving project quality through the establishment of a service quality management department.
9. Risks associated with product development quality	The Group has developed several in-house software products in the areas of institutional accounting, management accounting, business management, and data utilization platforms. In the development of new products and additions to existing products, we continuously strive to improve quality and prevent the occurrence of defects through development based on our management process. However we cannot deny the possibility that product defects may occur. Defects in our Group's products may affect our customers' operations, and failure to resolve such defects may cause a loss of trust in our Group, which may affect our Group's business performance and financial position.	To address this risk, we have established a product quality control department to reduce quality risk during product development.
10. Risks related to information security such as data loss and information leakage	In the course of our business activities, the Group may handle personal and confidential information of its affiliates and customers. There is a possibility that this information could be leaked due to unauthorized access to our Group's infrastructure from outside, leakage of information due to errors by our Group's officers and employees or contractors, or other unforeseen circumstances. Such an incident could have a serious impact on the social credibility of the Group and its customers, as well as on the Group's business performance and financial position.	To address this risk, we have established an Information Security Policy and a Personal Information Protection Policy to deal with security risks, and review these policies in response to advances in information and communication technology and changes in social conditions and the regulatory environment. The Information Security Committee, led by the Chief Information Security Officer (CISO) and headed by the President, has been established to formulate policies, implement measures, educate and enlighten employees, and conduct audits and evaluations. We have also acquired ISMS certification (ISO/IEC27001:2013), an international standard for objective evaluation and continuous improvement of these operations. We also conduct quarterly information security training to raise the security awareness of all executives, temporary employees, and outsourced employees.
11. Risks related to natural disasters	An eruption of Mt Fuji, flood damage from typhoons, storm surges, etc., could result in the loss of important information assets, a shortage of work-ready personnel, or the collapse of infrastructure, may make it impossible to resume business operations quickly. In addition, if our Group's business sites are damaged by natural disasters such as earthquakes or fires, and important documents and data related to business execution and intellectual property, etc. are lost, business activities may be hindered and our business performance and financial position may be affected.	To mitigate this risk, we are backing up important documents and data to a remote location, establishing an emergency headquarters and other initial response systems, and formulating a Business Continuity Plan (BCP) to resume business operations. In addition, by enhancing our online business infrastructure, we are striving to prepare for both the safety of our executives and business partners and the continuity of our business operations by utilizing remote work from normal times.

Compliance

In order to fulfill our responsibility for corporate organization and activities as a public institution of society, and to ensure the growth of our business and the continuous and efficient operation of our corporate organization, we have established the General Meeting of Shareholders as the highest body within the Company, and have designed the following organizational structure and internal control system.

- Establishment of a Board of Directors and selection a President and Representative Director to ensure accurate decision-making and speedy execution of operations
- Establishment of an Audit and Supervisory Committee, audit of the execution of duties by the Directors by the Audit and Supervisory Committee, election and dismissal of the Accounting Auditor, and determination of the content of proposals regarding non-reappointment of the Accounting Auditor
- Establishment of accounting auditors to ensure the appropriateness of financial reporting and internal controls through accounting audits and improve disclosure and information provision functions
- Response to important risks through the Risk Management Committee, Compliance Committee, and Information Security Committee, each of which includes the president, and ensuring compliance with laws, regulations, and rules, as well as information security

GROUP CRO MESSAGE

The Group has assigned a CRO and a Group Risk Management Department to oversee and promote risk management from the Group's perspective, and is promoting the strengthening of the risk management system. Group CRO Hiroki Takemura highlights our focus on strengthening risk management.

HIROKI TAKEMURA

Group CRO
Executive Vice President,
Diva Corporation

Our Risk Management System is an Important Means of Maximizing Business Opportunities and Achieving Sustainable Growth.

The Group positions risk management as a top priority item in order to achieve the new medium-term management plan and preserve the existing business base. Throughout the year, we maintain a Management Crisis List, with particular emphasis on risks from cyber attacks as a "significant important risk."

To address this risk, we promote control activities throughout the Group and regularly monitor and confirm their effectiveness. Cyber security is an unavoidable issue in today's age of digital transformation, and a prompt and appropriate response is essential for maintaining business continuity and customer trust.

In addition, we are also working to make continuous improvements by appropriately implementing a risk management cycle (PDCA) for other critical risks, such as investment and M&A risks, risks in securing and training human resources, and information security risks. Our risk management system is an important tool not only to avoid risk, but also to maximize business opportunities and achieve sustainable growth.