IT Strategies

Our Approach

SMBC Group is advancing both proactive and defensive digitalization initiatives to support efforts in its Seven Core Business Areas.

Proactive and Defensive Digitalization Initiatives

SMBC Group is moving forward with digitalization initiatives targeting four areas. Through proactive digitalization initiatives, the Group aims to (1) generate new businesses and (2) create customer benefits and business value through the transformation of existing business models. Under defensive digitalization initiatives, the Group seeks to (3) automate operations and processes in conventional businesses and (4) establish IT infrastructure to support medium- to long-term business reform.

Proactive digitalization initiatives include utilizing artificial intelligence, promoting cashless and other strategies. Meanwhile, defensive digitalization initiatives go beyond maintaining existing systems and ensuring stable operation to include IT transformation initiatives for adopting cutting-edge architectures. In these initiatives, we pursue efficient operations through the development of shared group-wide platforms and the utilization of cloud technologies while embracing state-of-the-art IT infrastructure and development technologies.

IT Investment Strategies

Under the previous Medium-Term Management Plan, SMBC Group completed the overhaul of large-scale systems through measures including the renewal of its core banking system platform and the implementation of a mutual backup function between data centers. Initiatives as part of the current Medium-Term Management Plan involves the increased allocation of IT budget to strategic investments for business innovation and the creation of new businesses through digitalization.

SMBC Group applies rigorous standards to the selection of system development projects while also assessing and verifying the benefits of these projects before and after in order to maximize those benefits. Specific targets for return on investment and key performance indicators must be set for all projects, and the degree to which these targets are accomplished will be reviewed over a five-year period after the completion of each project. Corrective measures will be implemented with regard to those systems that have not reached the appropriate performance levels. Even after the desired performance has been realized, the effectiveness of each system will be measured in terms of sufficiency, efficiency, stability, and utilization so that improvements can be implemented to systems that have suffered declines in effectiveness. This process constitutes a PDCA (plan-do-check-act) cycle that will be employed to maximize the benefits of IT investments.

Digital Governance and Sophisticated Human Resources Development

Under the guidance of the Group Chief Information Officer (CIO), we clarify lines of reporting for overseas offices and other Group companies in order to develop a corporate governance system that is integrated across the Group and globally. At the same time, we practice IT governance that emphasizes quality while evolving digital governance frameworks to

incorporate risk-based and speed-oriented perspectives for accelerating digitalization initiatives.

SMBC Group executes systematic personnel exchanges between the IT divisions of Group companies. In addition, the Digital University has been established within core IT Group company The Japan Research Institute, Limited, as an internal training institution for promoting IT adoption and digitalization. At the Digital University, we offer a unique menu of training programs including training based on the operations of specific Group companies, curricula employing the expertise gained from project case studies, and cutting-edge technology workshops.

Cyber Security

Cyber attacks are becoming ever-more serious and sophisticated. In order to respond to the risks of such attacks, SMBC Group has strengthened cyber security measures by defining cyber risks as one of its Top Risks and, establishing a Declaration of Cyber Security Management.

Seeking to facilitate management-led measures for fortifying response frameworks, the general manager of the System Risk Planning Department has been appointed as the Chief Information Security Officer (CISO). Positioned under the Group CIO and the Group Chief Risk Officer (CRO), the CISO has professional expertise regarding measures in this area, and steps have been taken to clarify the roles and responsibilities of CISO. Furthermore, we have established a computer security incident response team (CSIRT) and a security operation center (SOC), and analyses are performed on information regarding threats and observed phenomena collected from inside and outside of the Group. The results of these analyses, along with information on the status of security measures currently being implemented, are discussed regularly at meetings of the Board of Directors and the Management Committee to drive ongoing improvements to our cyber security measures.

The CSIRT is centered on the System Risk Planning Department, which possesses dedicated cyber security functions. To ensure preparedness for cyber incidents, the CSIRT coordinates with national government agencies as well as with the U.S. Financial Services Information Sharing and Analysis Center (FS-ISAC),*1 Financials ISAC Japan (Financials ISAC),*2 and other external institutions to share information on pertinent topics such as cyber attack methods and vulnerabilities.

The SOC, which is centered around The Japan Research Institute, is dedicated to continuously fortifying cyber security monitoring systems to mitigate the ever-rising threat of cyber attacks. Measures taken by SOC include the integration of the monitoring systems of Group companies and the development of global systems for conducting monitoring on a 24-hours-a-day, 365-days-a-year basis.

*1 An organization responsible for coordinating financial industry cyber security measures in the United States
*2 The Japanese equivalent of the FS-ISAC

SMBC Group's Cyber Security Governance System