IT Governance

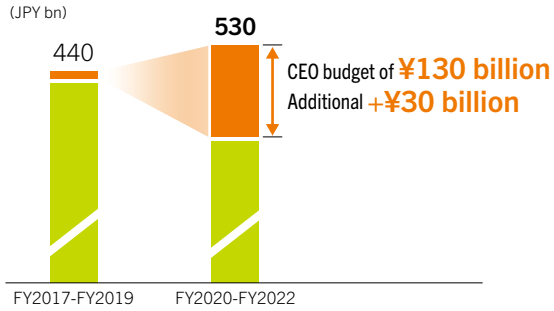
Our Approach

Currently, the operating environment for IT businesses is trending toward hybrid solutions, a maturing domestic market, growing overseas markets, the expansion of opportunities to utilize digital technologies, the reinforcement of security measures, the need for digital innovation/ digital transformations, and the importance of existing/BAU IT fields and IT system ownership and use. In this environment, we will advance IT strategies with a focus on supporting both management and business while also practicing effective IT governance.

IT Investment Strategies

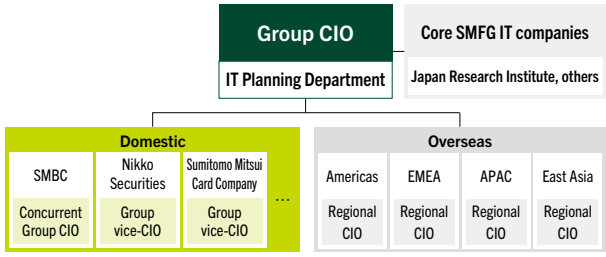
With the aim of fueling further growth of SMBC Group and to accelerate its digital strategy in Japan and overseas, we have increased the CEO budget by an additional ¥30 billion, bringing its total value to ¥130 billion. The CEO budget can be used to make flexible investments in fields in which Group CEO anticipates future growth. Total IT investment under the current Medium-Term Management Plan is ¥530 billion. Effective control of investments in existing IT areas is making it possible to allocate resources with an emphasis on strategic investments, such as promoting digitalization, reinforcing management foundations, building greater resilience and implementing business strategies.

Increased IT Investments for Future Growth



Group and Global IT Governance

We have a group IT governance structure in place to ensure that our IT systems comply with regulations that differ from business to business and from region to region, and to promote speedy strategies optimized for the group. Under the Group CIO, we have established vice-CIOs at SMBC Nikko



Securities and Sumitomo Mitsui Card Company, major Group companies in Japan, and regional CIOs in the Americas, EMEA, APAC, and East Asia, to operate effectively on both a group and global basis.

Digital Subsidiary Governance

SMBC Group has long promoted digital transformation, and has established a number of digital subsidiaries under the banner of "Producing New CEOs," with some services, such as eKYC of Polarify, now handling more than 10 million transactions annually. We are strengthening governance so that we can ensure the quality expected of SMBC Group without sacrificing the convenience of our digital services, while at the same time creating value through linkages with existing services.

Development of Human Resources for Supporting Sustainable Growth in a Digital Society

Accelerating digitalization at SMBC Group and contributing to customers and society require all employees, not just those in divisions dedicated to IT, to possess a digital-oriented mindset and basic IT knowledge. We have established the Digital University as an internal training institution for promoting training in IT and digitalization across SMBC Group. The Digital University provides training for all employees on digital IT literacy and on practical digital skills.

Much of its content is unique to SMBC Group, and includes curriculums utilizing know-how obtained from real system implementation projects as well as use cases for the latest technologies, making it possible to learn internal and external knowledge efficiently and systematically.

Cybersecurity

To address the risk of cyber threats that could seriously impact critical infrastructure and services, SMBC Group has greatly strengthened cybersecurity measures by defining such 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 Security Planning Department has been appointed as the Chief Information Security Officer (CISO), positioned under the Group CIO and the Group Chief Risk Officer (CRO), and steps have been taken to clarify the roles and responsibilities of the CISO in promoting strategies to counter the risk of cyber threats. Furthermore, we have established a computer security incident response team (CSIRT) and a security operation center (SOC) to ensure preparedness against evolving cyber threats, and analyses are performed on information regarding threats and observed incidents. The results of these analyses, along with information on the status of security measures are discussed regularly at meetings of the Board of Directors and the Management Committee.

The CSIRT is centered on the System Security Planning Department, which is exclusively responsible for cybersecurity. To ensure preparedness for cyber incidents, the CSIRT actively gathers information on attackers' methods and vulnerabilities from both within the Group and externally, and where necessary shares this information with national government agencies as well as with external institutions such as FS-ISAC* in the U.S. and ISAC* in Japan.

In order to prepare against the ever-growing risk of cyber threats, the SOC, which is centered on The Japan Research Institute, is working to strengthen its security monitoring systems by integrating the monitoring systems of Group companies, developing 24/7 global monitoring systems, and partnering with regional SOCs in Europe, the U.S. and Asia.

**Financial Services Information Sharing and Analysis Center*

SMBC Group's Cybersecurity Governance System