Cybersecurity

Basic Approach

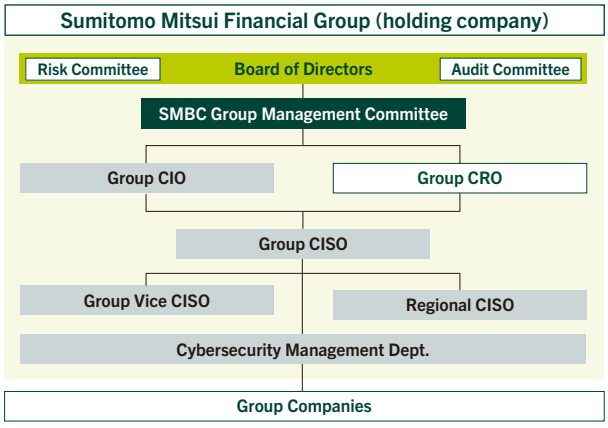
Amid accelerating digitalization and a changing environment for financial services, the posed by cyberthreats is growing increasingly serious. To provide safer, more secure services to customers and achieve a society that is resistant to cyber-threats, SMBC Group will further strengthen our cybersecurity.

Cybersecurity Management System

Viewing cybersecurity risks as one of the top risks faced by our management, we continuously engage in cybersecurity initiatives led by management under our "Declaration of Cybersecurity Management." We manage cybersecurity risks within the framework of company-wide risk management. The Cybersecurity Management Department, a dedicated department for cybersecurity, leads the formulation of basic policy on cybersecurity management, based on the external environment, business strategy, and other factors.

The SMBC Group Management Committee regularly deliberates to further strengthen cybersecurity management on the basis of the basic policy. In addition, the Board of Directors and internal committees such as the Risk Committee and the Audit Committee regularly deliberate cybersecurity management under the supervision of the Board of Directors.

SMBC Group's Cybersecurity Management System



To clarify the role of promoting effective cybersecurity measures, we have established the position of Group CISO*1 under the Group CIO and CRO. As the party responsible for general oversight of cybersecurity, the Group CISO engages in supervision and guidance for the development of Group and global system and the promotion of measures at sites from a professional perspective. Additionally, under the leadership of the Group CISO, we have appointed Group Vice CISOs and Regional CISOs, and have established a cybersecurity management structure encompassing over 700*2 professional staff on a Group and global basis.

1 Chief Information Security Officer
2 As of the end of March 2025

System for Responding to Cyber Incidents

We have established a CSIRT*3 in preparation for cyber incidents. The CSIRT actively collects information on attack vectors and on vulnerabilities within and outside the Group, and coordinates with national authorities and bodies such as U.S.-based FS-ISAC*4 and Financials ISAC Japan. We have also established a SOC*5, a dedicated organization for network monitoring and analysis, under a 24-hour, 365-day full-time monitoring system. Additionally, through close collaboration with SOCs established in Europe, the U.S., and Asia, we will further strengthen security surveillance on a Group and global basis.

3 Computer Security Incident Response Team
4 Financial Service Information Sharing and Analysis Center
5 Security Operation Center

See our website for more information on cybersecurity.
https://www.smfg.co.jp/company/organization/cybersecurity.html