IV. Cyber Security Management

1. Cyber Security Risk Management Architecture, Cyber Security Policy, Specific Management Plan, and Resources Invested in Information and Cyber Security Management

(1) Cyber security risk management architecture

A. Acting in accordance with Article 38-1 of the "Implementation Rules of Internal Audit and Internal Control System of Financial Holding Companies and Banking Industries," the Bank has appointed an SEVP to serve as its chief cyber security officer, and at its head office has established a Department of Cyber Security that is responsible for the Bank's cyber security operations, which include planning, monitoring, and implementation of cyber security management.

B. The Bank has established a Cyber Security Team that is chaired by its chief cyber security officer. This Team convenes periodic Meetings on Computer Security (two meetings in 2024). It is in charge of coordinating and setting the Bank's cyber security policies, plans, and resource allocations.

C. The Bank has adopted cyber security-related management systems. It has obtained ISO 27001 certification for its cyber security management system, ISO 22301 certification for its business continuity management system, and BS 10012 certification for its personal information management system. The Bank obtains validations by an impartial third party each year to keep these certifications current, to keep the Bank in line with the latest international trends in cyber security management, and to meet international management standards.

(2) Cyber Security Policy

The Bank has adopted a Cyber Security Policy which sets out the Bank's cyber security targets and cyber security work plans. The Cyber Security Policy is re-evaluated at least once per year to ensure that it complies with applicable laws and regulations, and to check whether recent changes in technology or the business environment require that it be updated.

(3) Resources invested in information and cyber security management

A. The Bank adopts and implements a cyber security maintenance plan every year, conducts a stocktaking of core and non-core business operations, adopts cyber security-related management systems and gets them approved by certification bodies, classifies its information and communication system defense requirements and sets system defense standards, and conducts business continuity exercises, security tests, and email social engineering drills.

B. The Bank has built a layered defense-in-depth system, which employs multiple technologies to defend against different types of attacks, thereby reducing security threats from the internet or an intranet and maintaining the confidentiality, integrity, and availability of important assets.

C. The Bank has set up mechanisms for detection and management of cyber threats, and promptly identify and deal with risks, in order to prevent problems before they occur.

D. The Bank conducts periodic vulnerability scans, penetration tests, and computer system and information system security assessments to discover potential cyber threats and vulnerabilities. In addition, the Bank conducts red team drills and security analyses to identify possible cyber security risks and strengthen the Bank's cyber defense capabilities.

E. The Bank conducts external corporate cyber risk ratings, uses an external perspective to assess BOT's cyber risks, confirms the degree of risk exposure generated by the organization's public-facing services, and carries out corrective action based on the ratings in order to improve cyber security.

F. The Bank continues to conduct email social engineering drills, the models of which more closely simulate environments in offices and everyday life. The purpose of the drills is to make Bank employees more alert to the dangers of social engineering.

G. Every year, the Bank uses training, internal conferences, posters, and other such methods to raise employee awareness of cyber security incidents and information regarding cyber security trends. The Bank also conducts periodic "Cyber Security Management Training Courses," "Workshops on Information Equipment and Cyber Defense," "Security Standards for Information Systems," "Workshops on FinTech Applications and Cyber Defense," and other such training programs to raise employees' cyber security consciousness. In addition, dedicated cyber security personnel must attend at least 15 hours of professional-level cyber security coursework to strengthen their cyber security expertise.

H. The Bank has established a cyber security incident notification mechanism, formulated related emergency response procedures, and used drills to implement adjustments and improvements on a rolling basis. If the Bank experiences any major cyber security incidents, the Chief Cyber Security Officer, who also chairs the Bank's Cyber Security Incident Response Team (CSIRT), takes charge of emergency response.