Information and Transaction Security

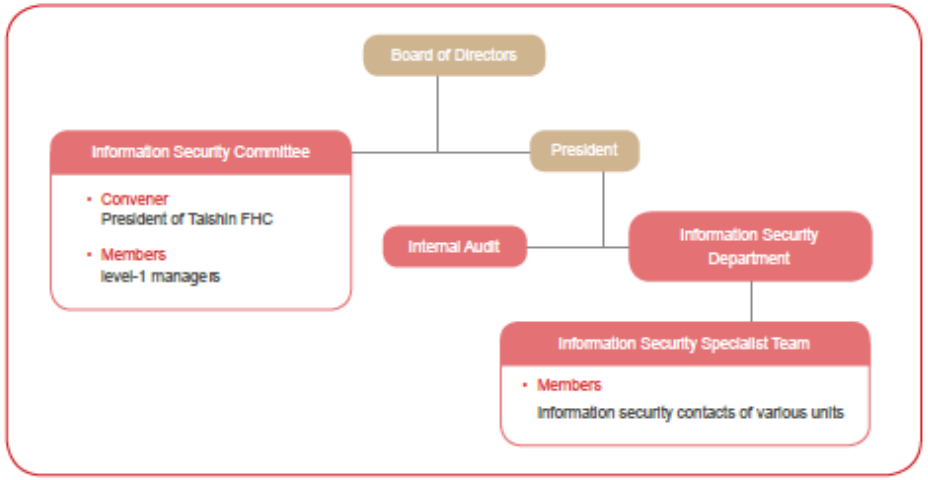
Information Security Management Mechanisms

Taishin FHC has implemented "Information Security Policy" and "Taishin Holdings Internet Security Management Guidelines" to serve as guiding principles for security protection. Meanwhile, an "Information Security Committee" comprising the Group President, Taishin Bank President and level-1 managers has been assembled within the organization. The committee holds quarterly meetings to discuss information security issues and improvement measures; and reports to board members on a yearly basis on issues concerning information security governance and planning.

An Information Security Department comprising employees from various fields of expertise was established in 2018 to oversee the planning and execution of Taishin Bank's information security policy. Meanwhile, an Information Security Department comprising employees who are information security contacts of various units has been established to facilitate more efficient management of information security risks from an organizational perspective. The Information Security Department oversees the information security management system and related internal and external issues and responds to stakeholders' requests. It coordinates with relevant departments to assess and manage related issues, and constantly searches for internal and external threats from a risk perspective to create an information security system that supports development of FinTech.

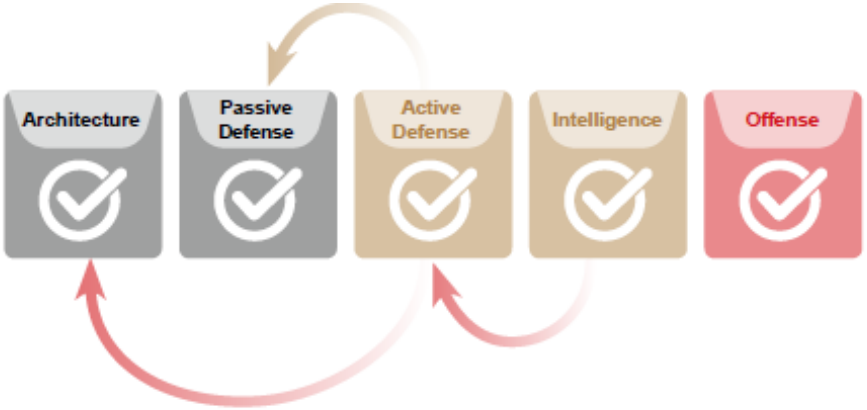
Taishin Bank first passed certification for ISO/IEC 27001 ISMS in 2010. Since then, the Bank has been engaging an independent third party to conduct half-yearly reviews and re-certification once every three years to optimize information security management, and thereby ensure effective functioning of the information security management system.

Framework of information security management



Upgraded Security Protection

Taishin Bank has created an extensive information security protection network that gathers security-related intelligence, such as hackers' attack and new trends, from around the world using available means at its disposal. In addition, the Bank constantly assesses its internal protections to determine whether they are adequate of ensuring timely response to the latest threats. All banking branches, including overseas branches, are subject to real-time virus protection and regular weakness scans and patching. Using in-depth defense and infrastructure protections, the Bank is able to patch up security weaknesses in a timely manner and thereby minimize risk of hackers' attack.

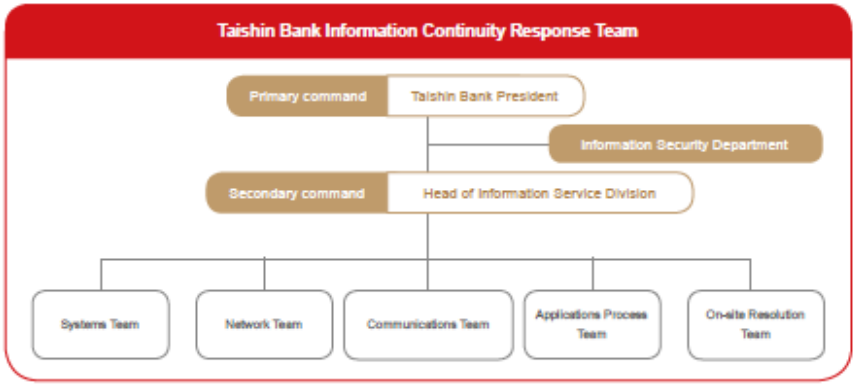


Information security risk management is currently executed as part of ISO/IEC 27001. The Bank gathers information security management issues from within and outside the organization, and engages various departments of the IT Division to assess the risks involved and potential impacts (sometimes at the request of stakeholders).

Compliance of Information Security Regulations

Given the increasing number of information security threats and attacks around the world, Taishin Bank has complied with laws of the home country and foreign countries where overseas branches are domiciled by conducting regular reviews and making regular reports to the local competent authority. In 2018, there had been no occurrence of information security-related or extraordinary incident that had to be reported to the local financial competent authority, and neither was there any compliance-related defect. Furthermore, no significant information security incident concerning customers' interest had occurred in the last 4 years.

Taishin Bank has assembled an information continuity response team according to the policy of the financial holding company to oversee real-time prevention and enhancement of information security. The response team is also responsible for gathering intelligence on new threats around the world and performing weakness analyses. If a threat arises, an information security threat alert will be disseminated immediately along with the activation of information security incident response procedures. In addition, Taishin's network security mechanism functions 24 hours a day and every day of the year to prevent hackers' intrusion.



Enhancement of Transaction Security

Given the severe losses suffered by banks around the world as a result of hackers' intrusion into the SWIFT system in 2017, Taishin Bank has since implemented several security protection measures for its information systems, network environment and ATMs, and will continue making enhancements to information security in the future. In addition, the Bank plans to improve its digital forensics capacity over the next three years and construct an information security monitoring center to further strengthen its security network for the protection of customer transaction security.

Transaction security mechanism

Global Digital Corporate Banking Network
Taishin has obtained multiple security certifications and adopted proper encryption mechanism to ensure that data is protected.

Mobile device
Using fingerprint/password for verification, Taishin is able to ensure the timeliness, convenience and security of new transaction tools including near-field contact and remote credit card.

Digital channel
Transaction verification mechanisms such as mobile device linkage, real-time SMS, transaction detection system etc are used for security purpose.

ATM whitelist
Taishin adopts the use of ATM whitelisting and reviews the list regularly to ensure the security of its ATM system.

Information security awareness and management of external parties

Information security awareness

All employees of the Bank must undergo at least 3 hours of information security awareness training and assessment each year. The training covers a broad variety of topics from regulations, operating procedures, IT equipment usage to information security incident studies, and is intended to develop proper information security awareness among employees. Training coverage and completion rates for 2018 were both 100%.

Social engineering drill

All employees of the Bank are required to undergo irregular social engineering drills, such as phishing email simulation, 4-6 times a year. Test results are further analyzed to identify employees with inadequate information security awareness, for whom the Bank will arrange additional training to address the weak link and minimize the risk of threat.

Information continuity drill

Major incidents involving key information systems are simulated on a yearly basis. By rehearsing response plans under different scenarios, the organization is able to make constant improvements to its system and data recovery processes, and thereby deliver more stable and reliable financial services for the protection of customer transaction security.

Supplier management

Taishin Bank has a set of "Information Service Outsourcing Guidelines" in place that outlines the standard operating procedures and rules concerning outsourcing of information service. The guidelines cover several issues including outsourced custody of computer hardware/ software, and outsourcing of information process and service. To ensure the safety and feasibility of outsourced processes, the project handler collaborates with employees from the IT Division to perform comprehensive and rigorous supplier assessments as well as risk assessments on selected vendors. Credit assessments are performed where appropriate to ensure the quality of internal processes and the vendor's ability to provide services in the best interest of the Bank and customers.

Vendor's criteria for outsourcing of major information processes

- Having adopted appropriate measures to ensure data security in customers' best interest.
- Having adopted appropriate measures to ensure the integrity of account data and transaction records.
- Having adopted appropriate measures, based on the sensitivity of the data and the transmission/storage method involved, to maintain the confidentiality of key information.
- Having adopted appropriate measures to protect customers' privacy with respect to the products and services offered.
- Having adequate capacity for the outsourced information system, and having developed an effective business continuity and disaster recovery plan to ensure the continuity of the information system and its service.
- Having implemented emergency procedures to ensure proper functioning of the information system and services.