Implementation Status of Information Security Management in Union Bank of Taiwan

Union Bank of Taiwan has established an "Information Security Policy" to strengthen information security across the entire bank, ensuring the security of data, systems, equipment, and networks. The overall goal of policy implementation is to maintain the confidentiality, integrity, and availability of the bank's information applications and prevent operational impacts due to information security incidents, thereby reducing potential operational risks. All personnel, data, application systems, hardware equipment, data centers, and network infrastructure must adhere to the bank's information security policy.

1. Bank-Wide Information Security Governance Organization and Structure

Board of Directors: The highest decision-making body for the bank's information security policy. The board includes directors with expertise in information technology and cybersecurity, responsible for reviewing and approving the bank's information security policy and overall implementation reports.

Our internal information security control adopts a three-line defense management structure:

- The **first line of defense** consists of the information technology (IT) department and all operational units, responsible for executing information security tasks.
- The **second line of defense** includes the information security unit, responsible for planning, monitoring, and implementing security policies; the legal affairs & compliance department, responsible for ensuring regulatory compliance; and the risk management department, responsible for information security risk management.
- The **third line of defense** is the audit department, which conducts security inspections and audits.

The IT Department has established a "Information Security Management Section" as a dedicated information security unit responsible for the bank-wide governance, planning, supervision, and implementation of cybersecurity measures. A Vice President is designated as the Chief Information Security Officer (CISO), overseeing the promotion and resource allocation of the bank’s information security policies.

2. Bank-Wide Information Security Control Policy

2.1 Adoption of International Information Security Standards

The bank has implemented the ISMS (Information Security Management System) and obtained ISO 27001:2022 certification. To enforce international information security standards, the following security management organizations are established:

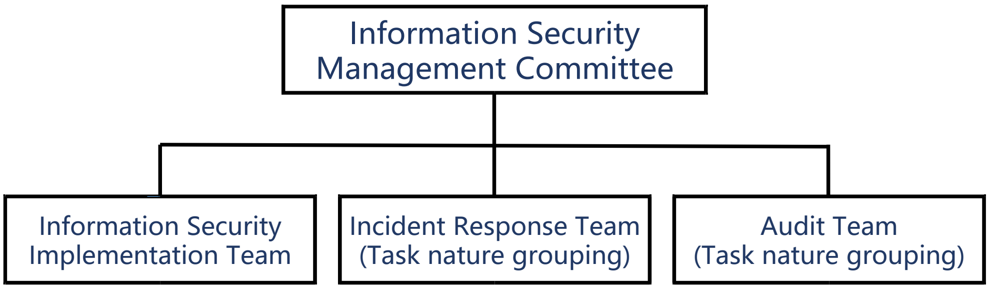

Information Security Management Committee
Information Security Implementation Team
Incident Response Team (Task nature grouping)
Audit Team (Task nature grouping)

Figure 1-ISMS Information Security Organizational Structure

- **Information Security Management Committee:** Led by the CISO, responsible for decision-making on security management systems and convening management review meetings.
- The Chief Information Security Officer shall serve as the convener and be responsible for deciding matters related to the information security management system and convening management review meetings.
- **Information Security Implementation Team:** Responsible for planning and executing various security operations.
- **Incident Response Team:** Handles emergency responses to major information security incidents.
- **Audit Team:** Conducts internal audits of the information security management system.

2.2 Information Security Management Operations

The bank follows the "Information Security Policy" and "ISMS Security Management System" to establish a comprehensive security framework, covering organization security, asset classification, personnel security, physical and environmental security, communication and operational security, access control, system development and maintenance, disaster recovery, and regulatory compliance. Regular security audits, network monitoring, and personnel security management are conducted to strengthen protection capabilities and mitigate security threats and losses.

Regularly hold "Information Security Management Review Meetings" to report and discuss the Bank's information security management status.

3. Risk Management in Information Security

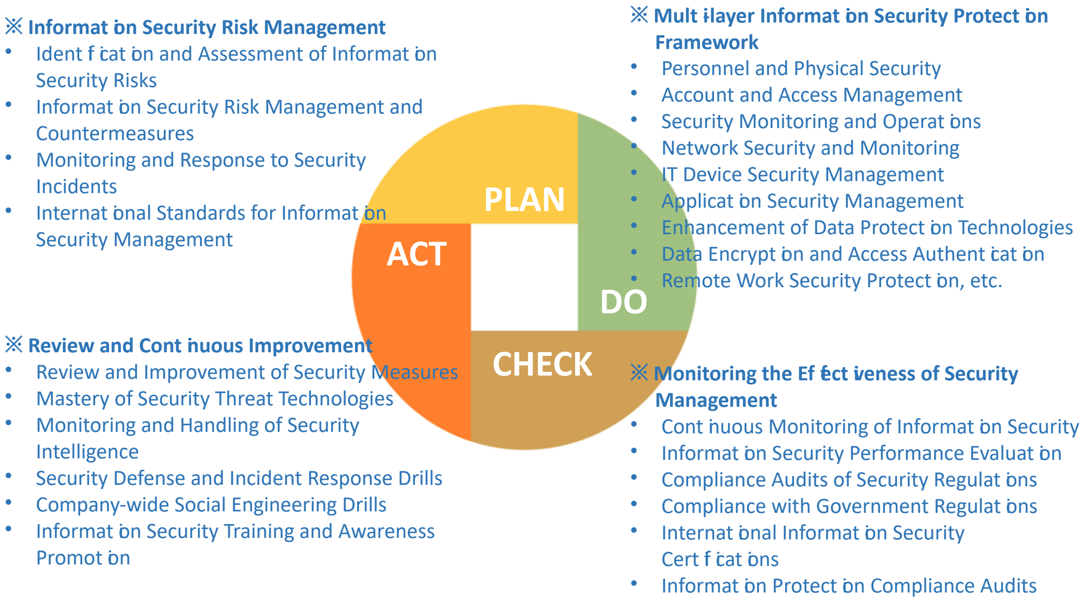
3.1 Information Security Assessments

To ensure the implementation of information security measures, our bank commissions a third-party professional organization each year to conduct an information security assessment and review the overall execution status. In accordance with the regulations set by the regulatory authorities and the self-regulatory standards established by industry associations, we examine the planning, monitoring, and execution of various information security management operations. Based on the assessment results, relevant reports are generated, and the overall execution status of information security is included in the internal control system statement, which is submitted to the Audit Committee and the Board of Directors for review and approval.

3.2 Information security risk management and continuous improvement cycle management framework

Following the ISMS framework, the bank implements a management cycle:

- **Plan:** Risk management, implementation of international security certifications, and systemic security threat reduction.
- **Do:** Multi-layered security defense, incorporating security controls into system operations, applications, and management workflows.
- **Check:** Reviewing security effectiveness through internal and external audits.
- **Action:** Continuous improvement, regular reviews, and security awareness training to ensure system and data protection.



※ Information Security Risk Management
- Identification and Assessment of Information Security Risks
- Information Security Risk Management and Countermeasures
- Monitoring and Response to Security Incidents
- International Standards for Information Security Management

※ Multilayer Information Security Protection Framework
- Personnel and Physical Security
- Account and Access Management
- Security Monitoring and Operations
- Network Security and Monitoring
- IT Device Security Management
- Application Security Management
- Enhancement of Data Protection Technologies
- Data Encryption and Access Authentication
- Remote Work Security Protection, etc.

※ Review and Continuous Improvement
- Review and Improvement of Security Measures
- Mastery of Security Threat Technologies
- Monitoring and Handling of Security Intelligence
- Security Defense and Incident Response Drills
- Company-wide Social Engineering Drills
- Information Security Training and Awareness Promotion

※ Monitoring the Effectiveness of Security Management
- Continuous Monitoring of Information Security
- Information Security Performance Evaluation
- Compliance Audits of Security Regulations
- Compliance with Government Regulations
- International Information Security Certifications
- Information Protection Compliance Audits

Figure 2-Information security control measures

3.3 Specific Measures for Information Security Management

(1) Monitoring and Early Warning of Information and Communication Systems

The bank implements real-time detection, monitoring, management, and early warning measures. It has deployed multi-layer firewalls, email filtering and auditing, spam filtering, phishing detection, web monitoring and protection, intrusion detection and prevention, antivirus detection and blocking, data leakage prevention, and threat intelligence monitoring equipment. Additionally, the bank has established a Security Information and Event Management (SIEM) system and an outsourced Security Operations Center (SOC) with 24/7 security monitoring to enhance security alert analysis, incident reporting, and response mechanisms.

(2) Application and Sharing of Cyber Threat Intelligence

The bank is a member of the Financial Information Sharing and Analysis Center (F-ISAC) and the Financial Security Operations Center (F-SOC), participating in the cybersecurity defense collaboration program. It actively receives and shares threat intelligence and adopts risk assessments and appropriate response measures based on the acquired intelligence to prevent cybersecurity incidents.

(3) Transaction Security Management and Data Protection

To ensure the security and accuracy of transaction data transmission, the bank continuously enhances system security design, adheres to industry association regulations, and implements security measures such as network segmentation, access control, and vulnerability management to strengthen security controls.

(4) Information Security Testing and Drills

The bank annually commissions external professional institutions to conduct various information security drills, including social engineering exercises, vulnerability scans, penetration testing, Distributed Denial-of-Service (DDoS) attack drills, and security assessments for applications and websites. These tests verify the effectiveness of security defenses and incident response capabilities, leading to vulnerability detection and remediation measures.

(5) Information Security Education and Training

In 2024, the bank's dedicated information security personnel each completed over 15 hours of professional cybersecurity or competency training, totaling 318 hours across seven staff members. All employees were required to complete a three-hour online cybersecurity awareness course and pass the corresponding test. Excluding 13 employees who were unable to attend due to exceptional circumstances or resignation, a total of 3,841 employees completed the training. In order to improve the security of IoT device management, we organized an education and training course for IoT device management personnel, and a total of 195 people from various units completed the course. In 2014, the company-wide participation and passing rate of the information security test was 100%.

(6) Information Security Incident Management

The bank has established an "Information Security Incident Management Policy" to handle security incidents. When a unit identifies a (suspected) security incident, it reports to the unit supervisor and the IT department's designated contact point to complete the internal notification process. The "Emergency Response Team" assesses the incident's impact, acceptable risk levels, and determines appropriate mitigation and control measures before carrying out further response actions.

(7) Outsourcing Management of Information and Communication Systems or Services

The bank manages outsourced information and communication system services in accordance with the "Regulations on Outsourcing Operations by Financial Institutions" and adheres to the "Guidelines for Managing External Information Service Providers."

(8) Implementation of Financial Cyber security Action Plan

To align with the Financial Supervisory Commission's (FSC) cybersecurity enhancement initiatives, the bank actively participates in and implements various security measures outlined in the action plan for financial institutions. The bank fosters a security-conscious organizational culture, strengthens cyber security governance capabilities, and ensures business continuity and data security, thereby enhancing its operational resilience.

3.4 Investment in Information Security Management

Annual investments in governance and technical security infrastructure, including:

- Strengthening security architecture and cybersecurity defenses.
- Cyber threat intelligence gathering and analysis.
- Employee security awareness training.

3.5 Implementation Results of the Bank's Enterprise Information Security Measures:

(1) Information Security Regulations

In 2024, 54 new or revised information security regulations were completed.

(2) Security Awareness Training

Developed training materials and recorded online courses for the 2024 information security training program, educating all employees on key information security regulations and best practices.

(3) Security Infrastructure Upgrades

Implemented new installations, replacements, and upgrades of various cybersecurity software and hardware systems.

(4) Remote Work Security

Established and effectively enforced information security protection mechanisms for remote and offsite work across all regions.

(5) Automated Data Backup

Implemented an automated data backup mechanism, ensuring daily backups are stored in an offsite data center, with periodic data recovery drills.

(6) Cybersecurity Testing and Protection

- In addition to firewalls, antivirus systems, and network monitoring tools, the bank conducts:
  - 4 vulnerability scans per year
  - 2 penetration tests per year
  - 1 Distributed Denial-of-Service (DDoS) attack simulation per year
- To mitigate the risk of service disruptions due to DDoS attacks, the bank is planning to establish a DDoS defense mechanism.
- In 2024, two social engineering exercises were conducted, involving 3,865 accounts per exercise. Employees who failed the test underwent social engineering awareness training, with 165 and 59 employees respectively completing the courses and tests, 98.5% of colleagues have security awareness of social engineering letters.

(7) Mobile Application Security Testing

The bank’s mobile applications were assessed by a certified security laboratory in accordance with financial institution security standards and successfully passed security tests.

(8) Anti-Phishing and Fraud Protection

Continued efforts in detecting and preventing phishing websites and fraudulent mobile applications impersonating the bank’s services.

(9) Employee Training & Security Awareness

- In addition to specialized training for cybersecurity personnel, all employees receive information security awareness training and participate in social engineering simulations.
- The bank has engaged professional institutions to offer secure coding training courses and established a consultation channel to enhance IT personnel’s secure development capabilities.
- In alignment with the Financial Supervisory Commission's (FSC) goal of encouraging financial institutions to employ security professionals with diverse expertise and internationally recognized certifications, 16 employees have obtained a total of 26 international cybersecurity certifications.

(10) Independent Security Assessments

Engaged independent third-party professional institutions to conduct security assessments, evaluating the effectiveness and security of existing controls to reduce cybersecurity risks.

(11) Threat Intelligence Sharing

Collaborated with F-ISAC (Financial Information Sharing and Analysis Center) to collect and share intelligence, ensuring awareness of the latest security trends and threats in the financial sector. A total of 231 pieces of threat and risk analysis have been completed in 2024.

(12) Participation in Financial Security Monitoring Initiatives

Joined the Financial Security Operations Center (F-SOC) Cybersecurity Defense Program to enhance collaborative cybersecurity defense efforts.

(13) Compliance with International Standards

- The bank’s IT department, including the information security unit, implemented the ISO/IEC 27001:2022 Information Security Management System (ISMS) in 2024 and obtained ISO/IEC 27001 certification.
- In September 2024, the bank conducted an expanded certification audit for its insurance agency business, with the certification valid from June 7, 2024, to June 6, 2027.
- The insurance agency business also adopted the ISO/IEC 27701 Privacy Information Management System (PIMS) in 2019 and continues to obtain periodic ISO/IEC 27701 certification, valid from June 7, 2024, to June 6, 2027.

3.6 Personal Data Protection Committee Structure

The bank has established a "Personal Data Management Committee" to oversee the effective operation of personal data protection policies, chaired by a Vice President appointed by the General Manager. Committee members include department heads from Corporate Banking, Business Management, Wealth Management, Credit Cards & Payment Services, Legal & Compliance, IT, and Risk Management. The committee supervises personal data protection, monitors regulatory compliance, reviews security incidents, and oversees related security projects.

4. Significant Cybersecurity Incidents and Responses

As of the most recent fiscal year and the publication date of this report, there have been no significant cybersecurity incidents resulting in financial losses or operational impact.