Contents

About this Report

01 Sustainability Strategy Blueprint

02 Climate

03 Health

04 Empowerment Strategy

05 Sustainable Finance

06 Sustainable Governance and Risk Management

6.1 Corporate Governance
6.2 Ethical Corporate Management
6.3 Risk Management
6.4 Information Security
6.5 Legal Compliance
6.6 Anti-Money Laundering, Combating the Financing of Terrorism and Countering Proliferation Financing
6.7 Service Quality and Customer Rights

07 Appendix

6.4 Information Security

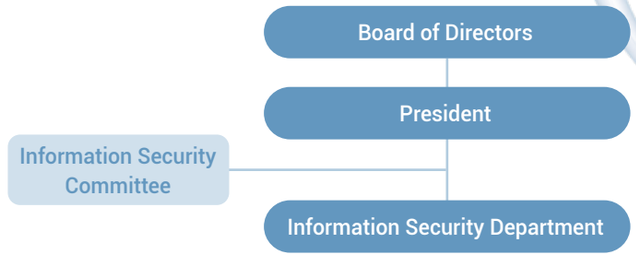
6.4.1 Information Security Management Policy

To enhance the quality and stability of financial services and effectively manage information security risks, CUB has established the Information Security Policy following the information security blueprint of its parent company, Cathay FHC. This policy serves as the guiding principle for implementing information security protection measures, continuously strengthening its information security capabilities, and achieving secure, convenient, and uninterrupted financial services.

The Bank has set up an Information Security Department as the dedicated unit responsible for monitoring compliance with information security laws and regulations, formulating the bank-wide information security policy, planning the information security architecture blueprint, coordinating the handling of major information security incidents, periodically reviewing information security defense mechanisms and emergency response plans. The Chief Information Security Officer (CISO), concurrently held by a Deputy General Manager or above, oversees policy implementation and resource allocation. The Information Security Department monitors the effectiveness of information security implementation across business units and promotes information security awareness programs and training. Through these actions, the Bank identifies information security risks and implements appropriate response measures.

In addition to the dedicated information security unit, the Bank has established a cross-unit Information Security Committee to ensure compliance with and promotion of information security policies and to supervise and coordinate information security management work. The President serves as Chairperson and the Chief Information Security Officer serves as Executive Secretary. Committee members include supervisors overseeing information technology, legal affairs, legal compliance, risk management, information security, and digital transformation. The committee meets at least once every six months and reports overall information security implementation to the Board of Directors annually. To keep pace with industry trends, emerging technologies, and cloud applications, the Bank continues to maintain international recognized third-party certifications, including ISO 27001:2022 and PCI DSS (Payment Card Industry Data Security Standard), in accordance with relevant laws, regulations, and self-regulatory rules. The Bank also achieved the ISO/IEC 27017 cloud-service information security management certification this year, becoming the first financial institution in Taiwan to obtain this certification for public cloud services.

Information Security Organizational Structure Chart



6.4.2 Information Security Action Plan and Achievements

The Bank regularly conducts computer system information security assessments, various contingency drills, penetration testing, cloud service security configuration assessments, intrusion and attack simulation drills, and white hat hacker red team drills, as well as enhanced testing of customer-facing service applications. Additionally, the Bank has established mechanisms for cyber threat intelligence collection and processing, a cybersecurity monitoring center, detection and takedown of fraudulent websites, and incident response mechanisms to ensure appropriate responses across all stages of emerging cybersecurity threats. In view of the growth of outsourcing and cross-industry cooperation in financial services, the Bank also continues to strengthen third-party information service provider management to prevent information security risks arising from the supply chain.

Furthermore, the Bank annually invests in cybersecurity insurance to ensure appropriate measures are in place against all new types of cybersecurity threat, protect its and its customers' interests, and minimize losses from cybersecurity incidents. This year, a total of NT$504.56 million was spent on cybersecurity expenses, including software and hardware licenses, personnel training, etc., accounting for approximately 37% of the Bank's total information budget of NT$1,372.31 million. The Bank also encourages employees to obtain cybersecurity certifications, with a total of 344 cybersecurity certifications achieved by the end of this year, covering both management and technical certifications.

Contents

About this Report

01 Sustainability Strategy Blueprint

02 Climate

03 Health

04 Empowerment Strategy

05 Sustainable Finance

06 Sustainable Governance and Risk Management

6.1 Corporate Governance
6.2 Ethical Corporate Management
6.3 Risk Management
6.4 Information Security
6.5 Legal Compliance
6.6 Anti-Money Laundering, Combating the Financing of Terrorism and Countering Proliferation Financing
6.7 Service Quality and Customer Rights

07 Appendix

Defensive measures for transaction systems and internal operations

The Bank's security controls include monitoring and defense against abnormal network traffic, network firewalls, web application firewalls, intrusion detection and prevention systems, as well as endpoint protection mechanisms (anti-virus and EDR). An Information Security Monitoring and Management Platform is established to aggregate security event logs from various security protection devices, and to centrally manage, store, search, and forward them to the Security Operation Center (SOC). This monitoring center provides 7×24 service and is responsible for analyzing and monitoring activities that may violate the confidentiality, integrity, or availability of information in the system. Once abnormal events are detected, they are immediately reported, processed, and tracked to ensure the security of transactions and the effectiveness of protection measures.

Implementing financial cybersecurity action plans

The Bank has completed the items required of financial institutions under the "Financial Cyber Security Action Plan 1.0" issued by the Financial Supervisory Commission on August 6, 2020, as well as the additional items added to the "Financial Cyber Security Action Plan 2.0" on December 27, 2022. In addition, based on the "Reference Guidelines for the Financial Industry's Adoption of a Zero Trust Architecture, " the Bank has formulated an implementation plan and continues to assess and expand adoption across various high-risk areas. The Bank also continues to strengthen its cybersecurity defense capabilities through cybersecurity maturity assessment tools, thereby achieving secure, convenient, and uninterrupted financial services.

Collaborated with third-party professional consultants to assess the implementation of information security both domestically and internationally

In order to enhance overall information security and comply with regulatory requirements in the financial industry, the Bank conducts regular computer system security assessments including the Bank's overseas branches every year. An independent professional consulting firm is engaged to evaluate the Bank's overall information security implementation annually. The assessment results, along with an internal control statement, are submitted to the Board of Directors before the end of the first quarter of the following year. Additionally, to gain deeper insights into the information security practices at overseas branches, information security personnel, along with third-party consultants, conduct on-site inspections. This ensures that operations at overseas branches comply with information security regulations and adhere to various security control requirements, aiming to embed information security into the corporate culture and enhance the Bank's overall security posture.

6.4.3 Information Security Training

The Bank conducts information security training every year. Training targets are divided into three categories—general employees, dedicated information security personnel, and Board members—with a focus on continuously strengthening information security awareness, professional skills, and the information security oversight capabilities of management.

Item	General Personnel Information Security Training	Information Security Personnel Training	Board Member Information Security Training
Total Number of Trainees	12,226	32	15
Completion Rate	100%	100%	100%
Total Training Hours	36,678	2,263	15