Financial Cybersecurity Action Plan 2.0: Progress Report

Data as of December 31, 2025

I. Introduction

The financial industry is characterized by an extensive use of information technology. Business models are continually being transformed by the introduction of digital processes, big data, and artificial intelligence, which in turn deliver great convenience to customers. However, as cybersecurity threats grow increasingly severe, the mindset toward financial cybersecurity protection must adapt rapidly. In response, the FSC, having taken note of international financial cybersecurity conditions and regulatory trends, released the initial Financial Cybersecurity Action Plan on August 6, 2020. After a continuous review that addressed business developments and technological advancements, the Financial Cybersecurity Action Plan 2.0 was released on December 27, 2022. This plan serves as a guiding framework for all financial institutions and industry associations against which to measure their cybersecurity strategies, management systems, and protective technologies, with the ultimate goal of providing secure, convenient, and uninterrupted financial services.

Building upon previous strategic initiatives, the Financial Cybersecurity Action Plan 2.0 considers cybersecurity through the lens of four key dimensions: strengthening regulatory supervision, enhancing cybersecurity governance in financial institutions, solidifying operational resilience, and optimizing joint defense capabilities. The plan offers 40 specific cybersecurity measures to expand applicability, ensure a thorough implementation, and foster foresight so as to achieve continuous improvement.

Given the comprehensive scope of this initiative, the FSC will bring together relevant resources and implement the plan progressively over a three-year period. Execution strategies will feature public-private partnerships, differentiated management, resource sharing, incentive mechanisms, and international cooperation. Furthermore, outcomes will be reviewed on a quarterly basis, allowing for dynamic adjustments to the plan in response to emerging cybersecurity trends and operational realities.

II. Implementation Status of Key Measures in Financial Cybersecurity

Action Plan 2.0

A. Strengthening Regulatory Supervision

1. Shaping a Cybersecurity-conscious Organizational Culture in Financial Institutions

(1) The FSC has mandated that financial institutions establish dedicated cybersecurity units and have the state of cybersecurity reported regularly to boards of directors. To enhance decision-making on cybersecurity issues, institutions of a certain scale or with a significant volume of electronic transactions are required to appoint a Chief Information Security Officer (CISO) at the vice president level or above to oversee the promotion and coordination of cybersecurity policies and resource allocation. Following amendments in September 2021 to the "Implementation Rules of Internal Audit and Internal Control System of Financial Holding Companies and Banking Industries," the "Regulations Governing Implementation of Internal Control and Auditing System of Insurance Enterprises," and the "Regulations Governing the Establishment of Internal Control Systems by Service Enterprises in Securities and Futures Markets," all domestic banks, securities firms with capital exceeding NT$10 billion or having a high proportion of electronic orders, and insurance companies with total assets exceeding NT$1 trillion in the previous year were required to appoint a CISO. On January 4, 2024, the scope was expanded for securities firms to require those firms with capital of NT$4 billion or more or meeting specific electronic trading criteria to appoint a CISO. As of Q4 2025, 39 banking institutions (including Chunghwa Post), 26 securities firms, and 12 insurance companies had appointed a CISO.

(2) Financial institutions are encouraged to appoint directors or advisors with a cybersecurity background or to establish cybersecurity advisory committees. This measure aims to integrate professional expertise into board operations and foster a security-conscious organizational culture. As of Q4 2025, 31 financial institutions had appointed directors with a cybersecurity background, 36 had hired cybersecurity advisors, and 32 had established cybersecurity advisory committees.

(3) Cybersecurity training courses are held for directors and supervisors to improve their understanding of the cybersecurity landscape and ensure that cybersecurity risks are treated as a key factor in strategic business decisions. In 2023, training organizations conducted 51 courses

attended by 724 people. In 2024, 41 courses attracted 677 attendees. And through Q4 2025, 55 courses had been conducted for 1,157 attendees.

(4) The capabilities of CISOs are being improved through regular liaison meetings and major cybersecurity incident response drills. These also serve as opportunities to discuss security trends, strategic initiatives, and key issues.

2. Broadening the Scope of Self-regulatory Norms

The FSC supervises financial industry associations as they amend and revise self-regulatory norms related to cybersecurity. This provides financial institutions with a basis for improving cybersecurity protection. Among these efforts are updating standards for information security protection, cybersecurity regulations concerning emerging financial technologies, and supply chain risk management regulations. The FSC has also overseen the establishment of standards mapping digital identity verification levels to business risks, aiming to strike a balance between innovation and security while meeting practical operational requirements. As of Q4 2025, nine self-regulatory norms have been amended or revised, as follows:

- Cybersecurity Protection Standards for Financial Institutions
- Regulations Governing Security Operations for Automatic Teller Machines Systems Provided by Financial Institutions
- Regulations Governing the Use of Artificial Intelligence Technologies by Financial Institutions
- Taiwan Securities Association Emerging Technology Cyber Security Self-regulatory Rules
- Chinese National Futures Association Self-Regulatory Regulations on Information and Communication Security in Emerging Technologies
- Taiwan Securities Association Self-regulations Governing Supply Chain Risk Management
- Chinese National Futures Association Self-Regulatory Regulations on Information System and Service Supply Chain Risk Management in the Futures Industry
- Regulations Governing Risk Management of Information Systems and Service Supply Chains for Financial Institutions
- Self-Regulatory Rules for Conducting Digital Identity Authentication by Insurance Enterprises

3. Bolstering Financial Cybersecurity Examinations

The purpose of financial cybersecurity examinations is to drive the effective implementation of security measures by financial institutions. To adapt to the changing ICT environment and emerging technologies in financial services, the FSC annually reviews and adjusts the focus of its cybersecurity examinations to enhance their comprehensiveness and effectiveness. Furthermore, to advance the practical effect of these examinations, the FSC provides professional training for examiners to help them keep pace with evolving threats and technologies by continuously enhancing their professional capabilities.

B. Enhancing Cybersecurity Governance in Financial Institutions

1. Enhancing Cybersecurity Management

(1) **Strengthening Cybersecurity Management**: To ensure that financial institutions can review their information security management systems holistically, establish a virtuous cycle of improvement, and identify blind spots through third-party validation, the FSC has directed industry associations to define the scope for adopting international cybersecurity management standards tailored to each sector. As of Q4 2025, 39 banking institutions (including Chunghwa Post), 22 securities firms, and 37 insurance companies had obtained international standard certifications of ISO 27001.

(2) **Assessing Governance Maturity:** The FSC has adapted the US Federal Financial Institutions Examination Council's (FFIEC) Cybersecurity Assessment Tool (CAT) for use in Taiwan's financial sector. Institutions are encouraged to use this framework to conduct self-assessments of their cybersecurity vulnerabilities based on their unique risk profiles and to continuously strengthen cybersecurity management. As of Q4 2025, 34 banking institutions (including Chunghwa Post), 25 securities firms, and 30 insurance companies had conducted these assessments.

2. Enhancing Cybersecurity Monitoring and Protection

(1) **Creating Security Operations Center (SOC) :** The timeliness and effectiveness of detecting and providing alerts on anomalous network behavior are critical for nipping threats in the bud and limiting damage. The FSC has promoted the establishment of Security Operations

Centers (SOCs) within financial institutions as these can play a key role in early detection and enable a shift toward proactive defense. As of Q4 2025, 39 banking institutions (including Chunghwa Post), 35 securities firms, and 38 insurance companies had established SOCs.

(2) **Effectiveness Evaluation:** Cybersecurity demands early detection and response, and a defensive posture will leave gaps. To ensure monitoring and protection measures are robust, institutions that have established SOCs are encouraged to instead adopt an attacker's mindset. By regularly conducting exercises such as DDoS exercises, red/blue team exercises, and Breach and Attack Simulation (BAS), they can test the effectiveness of their security monitoring and defense deployments. As of Q4 2025, 36 institutions had planned or conducted BAS, 83 had conducted DDoS exercises, and 41 had conducted red/blue team exercises.

3. Enhancing Cybersecurity Talent Cultivation

(1) The FSC coordinates with training organizations to offer specialized courses based on the talent competency map and practical industry needs. These courses help cybersecurity personnel enhance their knowledge and skills. In 2023, the 147 courses offered were attended by 5,604 individuals. In 2024, the 109 courses offered were attended by 3,593 people. And through Q4 2025, 114 courses had been conducted that saw 4,052 attendees.

(2) Financial institutions are encouraged to employ cybersecurity personnel with diverse skills who have obtained international cybersecurity certifications. This enhances the institution's defense capabilities while also supporting the career development of cybersecurity talent. As of Q4 2025, 39 banking institutions (including Chunghwa Post), 63 securities firms, and 38 insurance companies employed personnel with international cybersecurity certifications. A total of 1,289 individuals held 2,751 certifications, an increase of 127 people and 435 certifications since the end of 2024.

C. Solidifying Operational Resilience

1. Enhancing Business Continuity Management Capabilities of Financial Institutions

(1) **Resilience Guidelines:** Recognizing that the disruption of financial information systems could undermine public confidence and financial

stability, the FSC has drawn on the policies of the UK, US, and EU, and has directed industry associations to establish operational resilience guidelines that include key components such as the identification of core business services, setting maximum tolerable disruption times, disaster response operations, stress testing, and validation of recovery capabilities.

(2) **International BCM Standards:** To promote a standardized framework for business continuity management (BCM), institutions are encouraged to adopt international BCM standards. This allows them to follow best practices and use third-party verification to demonstrate compliance with internal, regulatory, and customer requirements and to communicate the institution's preparedness for potential impacts to its stakeholders. As of Q4 2025, 23 banking institutions (including Chunghwa Post), 9 securities firms, and 15 insurance companies had obtained international BCM standard certifications.

(3) **Live Drills:** To verify that off-site backup and recovery mechanisms are effective during a crisis, institutions are encouraged to conduct live operational continuity drills that include the validation of actual business operations. As of Q4 2025, 28 banks, 40 securities firms, and 23 insurance companies had conducted such drills.

2. Strengthening Cybersecurity Exercises:

Following the practice of European and US regulators, the FSC promotes the use of penetration testing and adversarial simulations to strengthen the incident response capabilities of financial institutions. Based on international threat intelligence and the results of previous exercises, exercises are planned to test and enhance the real-world defense and response capabilities of institutions. In 2024 and 2025, various activities were conducted, including DDoS defense exercises, cybersecurity attack and defense training courses, financial cybersecurity attack and defense competitions, and major cybersecurity incident response scenario exercises.

D. Optimizing Joint Defense Capabilities

1. Cybersecurity Intelligence Sharing and Cooperation

(1) The FSC supervises the Financial Information Service Co., Ltd. in its operation of the Financial Information Sharing and Analysis Center (F-

ISAC). F-ISAC enhances the depth and breadth of intelligence analysis and provides services including information sharing, a financial Computer Emergency Response Team (CERT), and joint defense SOC. As of Q4 2025, F-ISAC membership included 326 institutions, including all major financial institutions supervised by the FSC.

(2) To deepen intelligence exchanges, F-ISAC encourages active sharing among its members to ensure that warnings are early and accurate. Through Q4 2025, F-ISAC issued 594 intelligence reports, of which 422 (71%) originated from member contributions that were subsequently analyzed and disseminated by F-ISAC. This demonstrates a strong, trust-based, two-way sharing mechanism.

(3) Recognizing that cyberattacks are borderless, F-ISAC actively engages in international collaboration. Since its establishment, the organization has joined the US FS-ISAC as a member, attended the attended the EU FI-ISAC annual conference, and signed a memorandum of understanding (MOU) with Japan's F-ISAC. It has since continued to expand its global network, signing an MOU with Thailand's TB-CERT in 2021, becoming a member of the Forum of Incident Response and Security Teams (FIRST) in 2022, and joining the Asia Pacific Computer Emergency Response Team (APCERT) in 2023.

2. Establishing a Financial Cybersecurity Incident Response System

Given the time-critical nature of incident response and the limitations of a single institution's resources, the FSC has promoted a multi-layered support structure. This system, which consists of financial holding company groups, industry associations, the Securities and Futures Computer Emergency Response Team (SF-CERT), and F-ISAC, is designed to assist individual financial institutions in managing and responding to cybersecurity incidents effectively.

3. Establishing a Financial Cybersecurity Monitoring System

In addition to encouraging individual institutions to build their own SOCs for early detection of anomalous network activity, the FSC has directed F-ISAC to establish a joint defense SOC, establish cybersecurity monitoring operational standards, and promote the adoption of monitoring configuration baselines and operational guidelines. The system enhances coordination between individual and joint SOCs, creating a comprehensive cybersecurity monitoring network

that can effectively correlate and analyze sector-wide security risks to strengthen overall defense. As of Q4 2025, 77 financial institutions were participating in the joint defense SOC operations.

III. Conclusion

Since the Financial Cybersecurity Action Plan 1.0 and 2.0 were launched, over five years have passed. Through public-private partnerships with financial industry self-regulatory organizations, industry associations, and financial institutions, phased objectives have been achieved. Key accomplishments include:

- the widespread appointment of Chief Information Security Officers (CISOs) and the engagement of board members, advisors, or advisory groups with cybersecurity expertise
- the comprehensive revision and enhancement of cybersecurity self-regulatory norms guidelines and operational directives
- the implementation of international cybersecurity management standards across the industry
- the drafting of a detailed competency map to guide the development of cybersecurity talent
- the creation of robust SOC mechanisms and joint defense SOC
- the regular execution of offensive/defensive cybersecurity drills and competitions, and
- the development of a sophisticated cybersecurity incident response system.

To adapt to business evolution and technological advancement, the FSC launched the "Financial Operational Resilience on Cybersecurity Ecosystem Blueprint (FORCE-B)"[1] on December 30, 2025. The Blueprint is built upon a four-pillar framework: Targeted Governance, Holistic Protection, Ecosystem Collaborative Defense, and Robust Resilience. The goal is to build a Secure, Trusted, and Sustainably Innovative financial ecosystem in Taiwan.

[1] https://www.fsc.gov.tw/uploaddowndoc?file=News/202601281700340.pdf&filedisplay=Financial+Operational+Resilience+on+Cybersecurity+Ecosystem+Blueprint.pdf&flag=doc