Financial Operational Resilience on Cybersecurity Ecosystem Blueprint (FORCE-B)

Financial Supervisory Commission

December, 2025

Table of Contents

I. Foundations

The financial industry is the cornerstone of a nation's economy. In view of the rapid development of financial technology (FinTech) and of the innovation going on in the financial services sector, the Financial Supervisory Commission (FSC) recognized that information and communication security (cybersecurity) faces severe challenges. Consequently, the *Financial Cybersecurity Action Plan* was released in August 2020. Since then, the COVID-19 pandemic drove a digital transformation in the financial industry, intensifying the cybersecurity threat landscape. To ensure the continuous provision of secure, convenient, and stable financial services to the public amidst risks such as major disasters and geopolitics, the *Financial Cybersecurity Action Plan 2.0* was released in December 2022. This plan has helped lead the financial industry to hire Chief Information Security Officers (CISOs), appoint directors or consultants with cybersecurity backgrounds, or set up cybersecurity advisory groups, thereby enhancing cybersecurity supervisory capacity. The plan also promotes the adoption of international cybersecurity management standards by financial institutions, the establishment of cybersecurity security operations centers (SOC), joint defense mechanisms, and to improve the effectiveness through continuous offensive and defensive drills so as to create a proactive defense.

However, in recent years, the rapid development of technologies such as cloud computing, artificial intelligence (AI), and quantum computing has brought new types of cybersecurity risks. The intricate cooperative relationships and supplier relationships among financial institutions have, furthermore, made the risk landscape more opaque and difficult to assess. Faced with continuous and escalating cybersecurity threats, the FSC, in addition

to continuing to promote Zero Trust Architecture (ZTA) [expanding cybersecurity defense to include non-traditional areas such as remote work and cloud access, and deepening the breadth and depth of cybersecurity protection] has also observed that the international community is promoting resilience-oriented supervision. In this vein of thinking, the emphasis is on having financial institutions possess the ability to respond quickly and recover when hit by cyberattacks, operational interruptions, or other issues. Therefore, the FSC continues to implement the Financial Operational Resilience on Cybersecurity Ecosystem Blueprint (FORCE-B). Through a four-axis framework of targeted governance, holistic protection, ecosystem collaborative defense, and robust resilience, participants aim to construct a financial ecosystem that is predictable, defensible, and recoverable, ensuring that critical financial services can continue to operate even under extreme scenarios.

II. Global Cybersecurity Challenges and Trends

The World Economic Forum (WEF) *Global Cybersecurity Outlook 2025* [1] indicates that geopolitical tensions, increasing supply chain interdependence, and the applications and challenges brought by the rapid development of artificial intelligence (AI) are major factors complicating the cyber environment. State-sponsored threats have spread to attacks on critical infrastructure. Furthermore, as organizations increasingly concentrate on specific vendors, attacks or vulnerabilities on such players can trigger chain reactions, affecting the entire ecosystem. Therefore, the WEF suggests strengthening public-private cooperation and enhancing supply chain collaboration and transparency. It also calls on organizational leaders to adopt a security-first mentality, view cybersecurity as a strategic investment to ensure resilience against emerging threats,

[1] https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

and quantify cyber risks and their economic effects to align investments with core business objectives.

The US Office of the Comptroller of the Currency (OCC) released the *Cybersecurity and Financial System Resilience Report*[2] in July 2025, pointing out that major cyber threats to the financial industry include ransomware, distributed denial of service (DDoS) attacks, account takeovers, supply chain risks, geopolitical threats, AI threats, and post-quantum cryptography challenges.

According to the International Monetary Fund (IMF) *Global Financial Stability Report 2024*, a single cybersecurity incident could cause losses of up to USD 2.5 billion, or 800% of a typical financial company's operating income[3], potentially jeopardizing its solvency and capital adequacy. In an October 2025 report[4], it also pointed out that operational disruptions caused by cyberattacks could affect the functioning of foreign exchange markets, leading to liquidity crunches and severe market volatility. It emphasized that even a brief suspension of a trading platform would be sufficient to affect market liquidity and cause settlement delays, or even trigger cascading systemic pressures across markets.

Consequently, international bodies have launched more comprehensive and proactive strategies addressing regulatory policies, risk management, and defense technologies. The goal is to enhance the operational resilience of financial institutions in the face of extreme scenarios to maintain the long-term stable development of financial markets.

A. Increasing Senior Management Responsibility and Ensuring the Maturity of Cybersecurity Operations

[2] https://www.occ.treas.gov/publications-and-resources/publications/cybersecurity-and-financial-system-resilience/index-cybersecurity-and-financial-system-resilience-report.html
[3] https://www.elibrary.imf.org/display/book/9798400257704/CH003.xml
[4] https://www.imf.org/en/publications/gfsr/issues/2025/10/14/global-financial-stability-report-october-2025

The New York Department of Financial Services revised the *Cybersecurity Requirements for Financial Services Companies* (23 NYCRR Part 500)[5] in November 2023. In line with these regulations, the board of directors or an appropriate committee consisting of senior management and in possession of relevant expertise is to be made responsible for supervising cybersecurity risk management and regularly review and cybersecurity-related policies and reports. The rules also clarify the CISO's responsibilities, including regular reporting to senior management on cybersecurity implementation, immediate reporting of major cybersecurity issues, and joint signing of cybersecurity compliance certifications.

The US National Institute of Standards and Technology (NIST) released the *Cybersecurity Framework* (CSF) Version 2.0[6] on February 26, 2024. The framework adds a *Govern* function which permeates the entire framework and addresses six categories: *Organizational Context*, *Risk Management Strategy*, *Roles/Responsibilities/Authorities*, *Policy*, *Oversight*, and *Cybersecurity Supply Chain Risk Management*. Following this release, the Cyber Risk Institute (CRI), composed of financial institutions and industry associations, released the financial sector-specific *Cybersecurity Profile* Version 2.0[7] on February 29, 2024, designed to help the financial industry measure the maturity of its cybersecurity measures and manage risks through standardized questionnaires based on the CSF 2.0.

The European Union passed its *Digital Operational Resilience Act* (DORA)[8] in December 2022, which took effect on January 17, 2025. Article 5 of the DORA explicitly requires the management

[5] https://www.dfs.ny.gov/system/files/documents/2023/12/rf23_nycrr_part_500_amend02_20231101.pdf
[6] https://cyberriskinstitute.org/cri-issues-profile-version-2-0/
[7] https://cyberriskinstitute.org/the-profile/
[8] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554&from=FR

body (board of directors) of a company to bear final responsibility for information and communications technology (ICT) risk management and to undergo regular ICT-related training to ensure that they are sufficiently well versed in and therefore capable of assessing risk.

The Financial Services Agency (FSA) of Japan released its *Guidelines on Cybersecurity for the Financial Sector*[9] in October 2024, in which it pointed out that cybersecurity is not merely a technical issue for IT departments. Boards of directors and senior executives must lead policy formulation and resource allocation and bear the legal liability for losses caused by mismanagement. It also emphasizes that financial institutions should identify, assess, and mitigate cyber risks based on the business environment as well as their own strategies and risk tolerance, avoiding superficial efforts merely for the sake of compliance. It classifies response measures into *fundamental response measures*, which are basic practices all financial institutions should implement, and *recommended measures*, which are advanced best practices for large financial institutions and financial market infrastructures.

B. Promoting *Shift-Left* Security and Software Material Management

The NIST released the *Secure Software Development Framework* (SSDF)[10] in February 2022, pointing out that to ensure software is sufficiently secure, security practices should be implemented throughout the Software Development Life Cycle (SDLC). It divides secure software development into four aspects: *Prepare the Organization*, *Protect the Software*, *Produce Well-Secured Software*, and *Respond to Vulnerabilities*. It provides practical efforts and implementation examples for each category to

[9] https://www.fsa.go.jp/common/law/cybersecurity_guideline_en.pdf
[10] https://csrc.nist.gov/projects/ssdf

help organizations internalize cybersecurity as a part of software quality and *shifting left* cybersecurity issues to see them resolved in the earlier, lower-cost stages of the SDLC. It also notes that information on every software component (such as the Software Bill of Materials, SBOM) must be obtained during the production process to quickly and effectively respond to new vulnerabilities after software release. The Cybersecurity and Infrastructure Security Agency (CISA) released the white paper *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software* in October 2023 with 17 US and international cybersecurity agencies, proposing three core principles to help software manufacturers incorporate security into their design process and providing best practices for security by design[11].

As to managing software components, the *Payment Card Industry Data Security Standard* (PCI DSS) Version 4.0[12], released in 2022 (and taking effect March 31, 2024, while becoming mandatory from March 31, 2025), requires institutions affected by Clause 6.3.2 to maintain an inventory of custom software and third-party software components to facilitate vulnerability management and patching. CISA released the third version of *Framing Software Component Transparency*[13] in 2024, further defining the attributes and creation process of the SBOM as a common standard for software component information sharing. This, in turn, promotes software supply chain transparency and accountability. The EU's *Cyber Resilience Act* (CRA)[14] entered into force on December 10, 2024 (mandatory from 2027), also requiring that manufacturers of "products with digital elements" (including software) sold in the EU must record an SBOM to facilitate vulnerability tracking by

[11] https://www.cisa.gov/securebydesign
[12] https://www.commerce.uwo.ca/pdf/PCI-DSS-v4_0.pdf
[13] https://www.cisa.gov/resources-tools/resources/framing-software-component-transparency-2024
[14] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847

manufacturers and users.

C. Promoting AI Cybersecurity Governance and Protection

The UK National Cyber Security Centre (NCSC) released its *Guidelines for Secure AI System Development*[15] in November 2023, dividing the AI development lifecycle into four key areas: *Secure Design*, *Secure Development*, *Secure Deployment*, and *Secure Operation and Maintenance*. It proposes corresponding precautions and mitigation measures for each area to reduce the overall risk of the AI system development process. The UK Department for Science, Innovation and Technology (DSIT) subsequently released the *Code of Practice for AI Cyber Security* and the *Implementation Guide for the AI Cyber Security Code of Practice*[16] in January 2025.

The US NIST released the first version of the *Artificial Intelligence Risk Management Framework* (AI RMF)[17] on January 26, 2023, primarily describing methods for managing AI risks and pointing out security issues unique to AI systems. In January 2024, it released a report on adversarial machine learning[18], detailing attack types and mitigation methods against predictive and generative AI. In July 2024, it provided recommendations for risk management concerning generative AI[19].

The renowned non-profit organization OWASP (Open Web Application Security Project)[20] released the first version of its GenAI Security Project in October 2023, providing software developers with security recommendations for generative AI. Another renowned non-profit organization, MITRE, has also progressively added AI-related indicators to its ATT&CK (Adversarial Tactics, Techniques & Common Knowledge)

[15] https://www.ncsc.gov.uk/collection/guidelines-secure-ai-system-development
[16] https://www.gov.uk/government/publications/ai-cyber-security-code-of-practice
[17] https://www.nist.gov/itl/ai-risk-management-framework
[18] https://csrc.nist.gov/pubs/ai/100/2/e2023/final
[19] https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-generative-artificial-intelligence
[20] https://genai.owasp.org/

framework[21] since 2024.

The *EU Artificial Intelligence Act* (AI Act)[22] entered into force on August 1, 2024. Article 15 explicitly requires that high-risk AI systems must include appropriate security measures (Annex 3 points out that the financial sector may utilize AI systems to ascertain the creditworthiness of natural persons or to establish credit scores, while AI systems may be used for insurance assessments and pricing related to natural persons), and be able to withstand attacks by malicious third parties.

D. Planning for Post-Quantum Cryptography (PQC) Migration

The NIST and J.P. Morgan & Co. suggested in 2020 that the financial industry immediately establish crypto-agility[23]. The US president signed the *Quantum Computing Cybersecurity Preparedness Act* into law in December 2022. The act promotes the migration of encryption mechanisms in critical infrastructure and government agencies to Post-Quantum Cryptography (PQC) systems capable of handling quantum computer threats. In 2023, the CISA, the National Security Agency (NSA), and the NIST jointly proposed quantum migration steps recommendations[24]. The NIST released three global PQC algorithm standards between 2024 and 2025. The European Union Agency for Cybersecurity (ENISA), meanwhile, released a report[25] in October 2022 suggesting the adoption of hybrid mechanisms (PQC + traditional encryption) during the transition phase to avoid risks caused by the introduction of new algorithms.

The US FS-ISAC (Financial Services Information Sharing and Analysis Center) established a working group and released several

[21] https://atlas.mitre.org/
[22] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689
[23] https://www.nccoe.nist.gov/sites/default/files/2021-10/6-Yassir-NIST-%2020200819-8.pdf
[24] https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography
[25] https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study

reports concerning making inventories of infrastructure encryption technologies, PQC readiness roadmaps, building crypto-agility, and the effects of these technologies on the payment card industry[26]. The Monetary Authority of Singapore (MAS) issued an advisory to financial institutions in February 2024 that concerned the cybersecurity risks associated with quantum computing[27], including the need to make inventories of cryptographic assets, engage with third-party vendors, and plan migration timelines. In July 2024, the MAS released the Quantum Computing Programme[28], committing SGD 100 million to support innovation in quantum computing and AI.

E. Strengthening Supplier Management and Operational Resilience

US financial regulators (Federal Reserve Board, Federal Deposit Insurance Corporation, OCC) jointly released the *Interagency Guidance on Third-Party Relationships*[29] in June 2023, dividing the third-party risk management lifecycle into five stages: *Planning*, *Due Diligence and Third-Party Selection*, *Contract Negotiation*, *Ongoing Monitoring*, and *Termination*. The document describes risk management principles for each stage of the lifecycle and mentions that risk-based management measures should be adopted based on the criticality of the third party, explicitly stating that reliance on third parties does not absolve institutions of their legal and compliance responsibilities to customers.

Regarding third-party and supply chain risks, the Financial Stability Board (FSB) proposed a set of risk management tools[30] in December 2023 to help financial institutions identify critical third-

[26] https://www.fsisac.com/knowledge/pqc
[27] https://www.mas.gov.sg/regulation/circulars/advisory-on-addressing-the-cybersecurity-risks-associated-with-quantum
[28] https://www.mas.gov.sg/schemes-and-initiatives/quantum-computing-programme
[29] https://www.occ.gov/news-issuances/bulletins/2023/bulletin-2023-17.html
[30] https://www.fsb.org/2023/12/final-report-on-enhancing-third-party-risk-management-and-oversight-a-toolkit-for-financial-institutions-and-financial-authorities/

party services and manage potential risks throughout the lifecycle of third-party relationships. It also set standards for financial authorities to supervise, identify, and manage systemic risks, emphasizing the importance of cross-border regulatory cooperation and information sharing. Considering that incident reporting is a key tool for regulators to monitor operational disruptions, the FSB released the FIRE (Format for Incident Reporting Exchange) framework[31] in May 2025. This aims to establish a globally common format for financial operational incident reporting covering the complete lifecycle from incident initiation to closure, enabling regulators to share incident information through standardized data exchange.

The EU released the *Digital Operational Resilience Act* (DORA)[32] in December 2022, which took effect on January 17, 2025. It requires financial institutions to establish ICT risk management frameworks, immediately report major cybersecurity incidents, and test digital operational resilience. It also includes requirements for contracts between financial institutions and suppliers, ensuring that financial institutions have the ability to withstand, respond to, and recover from various ICT disruptions and threats.

In terms of practical drills, besides requiring financial institutions to conduct their own resilience testing, the international community continues to organize joint drills of various types to test the resilience of the financial industry under different scenarios. In 2024, for example, drills simulating cyberattacks included the UK's CBEST[33] and the EU's TIBER-EU[34]; drills simulating large-scale cross-institutional disruptions included the UK's SIMEX[35], the US

[31] https://www.fsb.org/2025/04/format-for-incident-reporting-exchange-fire-final-report/
[32] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554&from=FR
[33] https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector/2024-cbest-thematic
[34] https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html
[35] https://www.bankofengland.co.uk/news/2024/october/simex-24-testing-the-uk-financial-sector-resilience

Hamilton Series[36], and Singapore's Exercise Raffles[37]; operational stress tests included the UK's CORST[38] and the EU's CRST[39]. These drills not only verified whether financial institutions have sufficient manpower and resources to quickly respond to cyber threats and recover from interruptions, but also addressed cross-institution communication and coordination, management of liquidity crises, and mechanisms for maintaining market confidence.

III. Current Status of Financial Cybersecurity Promotion and Development Strategies

The financial sector is a critical component of Taiwan's critical infrastructure. To protect property rights and provide stable financial services, the FSC has promoted the *Financial Cyberecurity Action Plan* since the end of 2020. Many goals have been achieved and the results have been incorporated into routine operations, such as holding regular reviews of the effectiveness of cybersecurity risk factors linked to financial supervisory tools, adjusting cybersecurity inspection priorities in response to emerging businesses, and conducting rolling reviews and revisions of cybersecurity regulations. Most major financial institutions have obtained international cybersecurity management standard certifications, conducted cybersecurity governance maturity assessments, and established security operating centers (SOC). They have also created financial cybersecurity incident response systems involving financial holding groups, financial industry self-regulatory organizations or associations, and F-CERT. Additionally, regulations require financial institutions of a certain scale to appoint a Chief Information Security Officer (CISO) and hold regular CISO liaison meetings, achieving significant progress in promoting cybersecurity

[36] https://www.chicagofed.org/events/2025/midwest-cyber-workshop
[37] https://www.mas.gov.sg/news/media-releases/2024/business-continuity-exercise-to-bolster-financial-sector-operational-resilience
[38] https://www.bankofengland.co.uk/prudential-regulation/letter/2024/thematic-findings-2024-cyber-stress-test
[39] https://www.bankingsupervision.europa.eu/press/pr/date/2024/html/ssm.pr240726~06d5776a02.en.html

awareness in the financial industry and enhancing cybersecurity risk management. In terms of promoting cybersecurity cooperation and international exchanges, the FSC established the Financial Information Sharing and Analysis Center (F-ISAC) at the end of 2017. This has promoted cybersecurity intelligence sharing and cooperation within the financial industry, established joint defense SOC mechanisms, and successively joined US FS-ISAC as a member, attended the EU FI-ISAC annual meeting, signed MOUs with Japan's F-ISAC and Thailand's TB-CERT, became a member of the Forum of Incident Response and Security Teams (FIRST), and joined the Asia Pacific Computer Emergency Response Team (APCERT).

To continually enhance the cybersecurity protection and response capabilities of financial institutions, the FSC established the *Financial Cybersecurity Talent Competency Map*[40] in 2021 to cultivate talent. This opened up the field to cooperation with peripheral training institutions to hold specialized classes for financial cybersecurity talent development while encouraging financial institutions to value the allocation of various cybersecurity talents and the acquisition of cybersecurity certification. Regarding protection technology, the *Reference Guide for Introducing Zero Trust Architecture in the Financial Industry*[41] was released in July 2024. It suggests that financial institutions adopt a risk-based approach, prioritize high-risk, low-impact areas for pilot implementation, and progressively introduce relevant control measures. F-ISAC was also tasked with releasing the Financial Institution Configuration Baselines and Financial Cloud Cybersecurity Monitoring Baselines, providing references for financial institutions to establish monitoring mechanisms such as

[40] https://www.fsc.gov.tw/websitedowndoc?file=chfsc/202405061552070.pdf&filedisplay=金融資安人才職能地圖_11304 版.pdf
[41] https://www.fsc.gov.tw/websitedowndoc?file=chfsc/202410210854050.pdf&filedisplay=金融零信任架構參考指引.pdf

cybersecurity protection settings and monitoring rules. Furthermore, through continuous activities such as DDoS offensive and defensive drills, network offensive and defensive training courses, financial cybersecurity offensive and defensive competitions, and major cybersecurity incident response scenario exercises, the FSC verifies the defense energy and response capabilities of financial institutions against attacks and encourages the improvement of cybersecurity capabilities.

Given that the various information and communication security threats are becoming increasingly serious, Taiwan's *National Cybersecurity Strategy 2025: Cybersecurity is National Security*[42] proposes four national strategic pillars against external threats like state-level cybersecurity threats, emerging technology challenges, and rampant cybercrime: *Whole-of-Society Defense Resilience*, *Homeland Defense and Critical Infrastructure*, *Key Industries and Supply Chains*, and *Application and Security of AI*. Among principles that reach across these pillars, Robust Cyber Governance and Protection emphasizes that Zero Trust Architecture has become an indispensable part of cybersecurity governance in recent years. Through the concept of "never trust, always verify," the scope of damage caused by cyberattacks can be reduced. The document declares that operational resilience is another core element of cybersecurity governance and that realizing resilience involves promoting the transformation of core functions of critical systems towards offshore cloud backup, and strengthening off-site backup and redundancy design of infrastructure. Additionally, Taiwan's *National Cybersecurity Development Program (2025-2028)* [43] proposes execution measures for critical infrastructure, including cultivating high-level cybersecurity talent, strengthening

[42] https://www.president.gov.tw/Page/317/1870
[43] https://www-api.moda.gov.tw/File/Get/acs/zh-tw/tcWbCXvyTtLkaRY

cybersecurity threat monitoring, enhancing intelligence sharing, conducting on-site drills and audits, and implementing cybersecurity protection baselines for various fields.

In line with the *National Cybersecurity Strategy* and the *National Cybersecurity Development Program*, and as can be inferred from the aforementioned international trends, proactively and effectively facing dynamic cybersecurity threats above and beyond minimum compliance standards will require elevating cybersecurity issues to the corporate governance level and adopting monitorable, measurable, and growable methods to continuously make cybersecurity more mature. It will also require implementing security controls from the very beginning of the development and use of software. Financial institutions ought to change their traditional system-centric concern for business continuity towards a service-centric focus on operational resilience. In so doing, they ought to see the entire ecosystem (including suppliers and partners) as part of their service. Efforts will require preventing catastrophes as well as assuming that they will happen, necessitating constant testing and drilling against composite scenarios in order to effectively control risks, limit losses, and maintain reputation.

Therefore, this blueprint adopts a four-axis framework in seeking to guide the financial system to make a shift from being compliance oriented to being outcome oriented. The aim is to create a virtuous cycle of continuous improvement of cybersecurity governance, resulting in cybersecurity protection at financial institutions that is predictable, defensible, and recoverable.

	Axis	**Core objective**	**Achievement path**
A	Targeted governance	Outcome-oriented and strengthening decision and accountability chains to establish a measurable,	Increasing senior management accountability, adaptability to

	Axis	Core objective	Achievement path
		improvable governance system.	regulatory changes, and resilience of individuals.
B	Holistic protection	Protection along the entire chain from secure design to technical resilience, building a continuously evolving security technology roadmap.	Promote shift-left security and Zero Trust Architecture, enhance cybersecurity monitoring efficiency, and deploy an active defense concerning emerging technologies like AI and PQC.
C	Ecosystem collaborative defense	Build cross-domain joint defense and intelligent intelligence ecosystems to enhance the overall maturity of the cybersecurity ecosystem.	Strengthen supply chain cybersecurity management and intelligence analysis cooperation while furthering international joint defense measures.
D	Robust resilience	Ensure continuity and rapid recovery of critical services to achieve sustainable operation and rapid recovery.	Ensure critical financial services are uninterrupted through drills, backups, and risk layering.

IV. Promotion Measures

Based on the aforementioned four axes, 10 work items including 29 execution measures are being promoted:

A. Targeted Governance: Strengthening Decision-Making and Accountability Chains through an Outcome-Oriented Approach

Make the shift from being compliance-oriented to being

outcome-oriented, establishing a forward-looking and flexible cybersecurity governance model, strengthening senior management accountability, regulatory adaptation, and talent resilience, to build a governance system that is both measurable and improvable.

1. Strengthen Executive-Level Cybersecurity Governance and Accountability Mechanisms and Encourage Regulatory Adaptation

(1) Enhance Board Cybersecurity Supervision Capacity; Integrate Cybersecurity into the Core of Corporate Governance

The FSC requires financial institutions to report the implementation status of cybersecurity measures to their Board of Directors regularly. To enhance the Board's decision-making capacity regarding cybersecurity issues, the *Financial Cybersecurity Action Plan* encouraged financial institutions to appoint directors with cybersecurity backgrounds or set up cybersecurity advisory groups to include professionals in Board operations, to create an organizational culture that values cybersecurity. Looking ahead, the FSC will continue to promote enhancing the cybersecurity supervision capabilities of the Board, integrate cybersecurity into the core aspects of corporate governance, and align information security goals with the organization's overall business goals to ensure that cybersecurity strategies create value for the enterprise, reduce risks, and achieve sustainable development.

(2) Strengthen Financial CISO Accountability and Empowerment Mechanisms

The FSC has already been promoting the creation of the position of Chief Information Security Officer (CISO) at the

vice president level or above at financial institutions of a certain scale or having a certain proportion of electronic transactions. To further strengthen the duties and responsibilities of the CISO and ensure that such individuals have sufficient competence, resources, and authority to execute cybersecurity operations, the FSC will reference the US NYDFS Part 500 to clearly define the CISO's responsibilities. This includes having the CISO be partly responsible for the compliance of cybersecurity operations as well as for reporting the overall cybersecurity implementation status to the Board of Directors on an annual basis. Additionally, considering the differences in business, scale, and environment of each financial institution, the CISO will be appropriately authorized to adopt equivalent control measures based on certain reasons or with a specific scope during execution, thereby enhancing the efficiency and flexibility of cybersecurity governance. This aims to establish a financial cybersecurity governance architecture integrating responsibility, authority, and resources. It therefore enhances the accountability chain, ensuring decision-making independence and improving governance flexibility and resilience.

(3) Revise Cybersecurity Self-Regulatory Rules; Encourage Cybersecurity Regulatory Adaptation

Based on the *Financial Cybersecurity Action Plan*, the FSC continues to supervise financial industry associations to revise cybersecurity-related self-regulatory rules or operational guidelines in response to cybersecurity threats, business needs, and emerging technologies, providing a basis for financial institutions to strengthen cybersecurity protection. Furthermore, considering that cybersecurity

compliance requirements are becoming increasingly complex and that institutions struggle to keep up with rapidly evolving threats, the FSC encourages regulatory adaptation or forward-looking layouts as concerns overlaps, obstacles, or strategic goals in existing regulations when amendments are made. It also encourages the adoption of a risk-based approach, appropriately authorizing CISOs to adopt equivalent control measures based on certain reasons or with a specific scope during execution, so as to enhance the efficiency and flexibility of cybersecurity governance.

2. Enhance Cybersecurity Talent Development and Exchanges, Moving from a Common Baseline to Reach Strategic Goals

(4) Conduct a Rolling Revision of the Financial Cybersecurity Talent Competency Map; Encourage Optimization of Cybersecurity Competency Allocation and the Acquisition of Professional Certifications

The FSC established the *Financial Cybersecurity Talent Competency Map* in 2021. This opened up the field to cooperation with peripheral training institutions to hold specialized classes for financial cybersecurity talent development while encouraging financial institutions to value the allocation of various cybersecurity talents and the acquisition of cybersecurity certification. This makes financial institutions more competent while also benefiting the career development of financial cybersecurity talent. To respond to globalized and state-level cybersecurity threats, based on this foundation, the map will be revised on a rolling basis in response to the development of emerging technologies, financial policies, regulatory adaptations, and practical needs. Financial institutions are also encouraged to

reference the US NICE framework [44] and inventory the current distribution and gaps of financial cybersecurity talent, thereby optimizing allocation of cybersecurity competencies.

(5) Encourage the Sharing of Forward-Looking Planning and Best Practices

Since the establishment of F-ISAC at the end of 2017 to promote financial cybersecurity joint defense, the FSC has established horizontal links among financial institutions. Through activities such as cybersecurity intelligence sharing, network offensive and defensive drills, major cybersecurity incident scenario exercises, and the introduction of Zero Trust Architecture, the FSC has facilitated exchanges and garnered the feedback of the financial industry. The FSC also exchanges views on current important cybersecurity policies, supervisory priorities, cybersecurity situations, and joint defense at regular CISO liaison meetings. In conjunction with the promotion of target-oriented governance, the plan is to use this as a foundation to organize regular cross-institutional thematic forums, workshops, or case studies. Such events will bring together cross-institutional talent in the same field to jointly discuss forward-looking planning and best practices in financial cybersecurity, encouraging knowledge sharing and technical improvement among cybersecurity talent and serving as a key strategy for the transformation into target governance.

(6) Goal-Oriented: Bridging Protection Baselines with Best Practices

Cybersecurity regulations are based on common protection baselines (i.e., minimum cybersecurity compliance

[44] https://niccs.cisa.gov/tools/nice-framework

requirements). However, relying solely on compliance requirements as a line of defense is insufficient to meet the rapid evolution of cyberattacks. The FSC previously referenced the US FFIEC's repeatable Cybersecurity Assessment Tool (CAT)[45] to adapt and define maturity levels, encouraging financial institutions to conduct self-assessments and continuously strengthen relevant cybersecurity management operations. However, a review shows that current regulations and maturity indicators are not fully aligned. Therefore, the plan is to use existing cybersecurity regulations as a baseline and best practices as the goal, revising and establishing maturity level assessment indicators. This will guide financial institutions to shift from compliance-oriented to goal-oriented, establishing a supervisory framework that is measurable, growable, and differentiable.

B. Holistic Protection: From Secure Design to Technical Resilience

Promote shift-left security as well as Zero Trust Architecture, enhance cybersecurity monitoring efficiency, and deploy an active defense against emerging technologies like AI and PQC, and construct a continuously evolving security technology roadmap.

3. Shift-Left Security and Secure By Design

(7) Encourage Adoption of Software Secure Development, Testing, and Deployment Processes (CI/CD)

Traditional software development processes focus on deploying functions and meeting user needs, often postponing security testing until the testing phase or just before launch. This can result in security defects present in the initial design

[45] https://www.ffiec.gov/sites/default/files/media/resources/FFIEC_CAT_May_2017.pdf

not being discovered early, increasing potential cybersecurity risks. Moreover, discovering security vulnerabilities late in development or just prior to launch necessitates emergency patches or mitigation measures, increasing repair costs and delaying project schedules. Therefore, the plan is to reference the US NIST SSDF framewor[46], the international organization OWASP SAMM model[47], and related application security verification standards (such as OWASP ASVS). This will encourage financial institutions to introduce secure development, testing, and deployment processes for their software. Institutions are to conduct risk assessments or threat modeling during the analysis and design phase, embed security controls into the design, development, testing, and deployment processes, adhere to secure development principles during implementation and testing, and appropriately integrate security tools (SAST/DAST) into subsequent release and deployment (CI/CD) pipelines.

(8) Establish Software Supply Chain Transparency and Vulnerability Tracking Mechanisms

Throughout the software lifecycle, utilize software composition analysis (SCA) tools to identify the components being used (including open source and third-party components) and their dependencies, generating an SBOM. This enhances software component transparency and traceability. By linking with vulnerability databases (CVE)[48] or known exploited vulnerabilities (CISA KEV)[49], a mechanism for vulnerability monitoring and version updates will be established.

[46] https://csrc.nist.gov/projects/ssdf
[47] https://owasp.org/2020/02/11/SAMM-v2
[48] https://www.cvedetails.com/
[49] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

(9) Develop API Security Baselines and Establish API Security Management Mechanisms

Considering that APIs are important bridges for communication between financial industry systems and often contain high privileges and risks, and noting that OWASP has released the Top 10 API Security Risks[50], the plan is to develop more complete API security baselines to cover partner APIs and internal APIs based on the Bankers Association's existing open API standards. Based on the sensitivity of accessed data and the accessing objects, API categories and levels will be distinguished to implement API cybersecurity controls.

4. Promote Zero-Trust Architecture to Elevate Cybersecurity Defense Baselines

(10) Promote Introduction in High-Risk Areas; Progressively Enhance Maturity

The FSC released the *Reference Guide for Introducing Zero Trust Architecture in the Financial Industry*[51] on July 15, 2024. The document advises financial institutions to adopt a risk-based approach and select high-risk, low-impact areas for pilot implementation. Based on the complete access path of a high-risk area (i.e., the five pillars *Identity*, *Devices*, *Networks*, *Applications*, and *Data*), institutions should assess the completeness of existing cybersecurity protection mechanisms and progressively introduce relevant control measures in four stages: *Traditional*, *Initial*, *Advanced*, and *Optimal*. According to a survey, through 2025, most financial institutions have selected areas to introduce or plan Zero Trust Architecture. Based on such a foundation, the FSC will

[50] https://owasp.org/www-project-api-security/
[51] https://www.fsc.gov.tw/websitedowndoc?file=chfsc/202410210854050.pdf&filedisplay=金融業導入零信任架構參考指引.pdf

continue to promote priority introduction in high-risk areas and progressively enhance maturity.

(11) Encourage Sharing and Exchange of Implementation Practices

To promote the introduction of Zero Trust Architecture in financial institutions, pilot groups composed of key promotion targets in various sectors will continue to be formed. F-ISAC will assist in establishing an exchange platform to conduct technical exchanges on Zero Trust Architecture, sharing implementation planning and practices, thereby driving continuous deepening and diffusion.

(12) Establish Consensus on Implementation Practices; Progressively Incorporate these into Basic Regulations

The FSC will regularly survey the implementation planning and progress of Zero Trust Architecture at various financial institutions. It will bring together relevant financial industry self-regulatory organizations and industry associations to jointly measure actual cybersecurity protection needs and execution feasibility based on the attributes, scale, and business risks of various financial sectors. The promotion strategy and implementation schedule will be revised on a rolling basis, and the assessment of the progressive incorporation of implementation reference principles into basic cybersecurity regulations will be conducted to raise the overall cybersecurity defense level.

5. Ensure the Greater Effectiveness of Cybersecurity Monitoring and Protection Measures

(13) Revise Cybersecurity Configuration and Monitoring Operational Baselines

The timeliness and effectiveness of network anomaly detection and alerts are critical to determining whether an anomaly escalates into a cybersecurity incident thus necessitating subsequent damage control. Since 2020, the FSC has encouraged financial institutions to establish SOC. In the following year (2021), it analyzed attack methods used by hacker organizations to formulate financial cybersecurity monitoring and configuration baselines as reference for financial institutions to configure their ICT equipment and establish operational SOCs, thus forming a mutually beneficial ecosystem involving F-ISAC, financial institutions, and ICT equipment manufacturers.

With the introduction and maturity enhancement of Zero Trust Architecture, cybersecurity monitoring and configuration baselines have become indispensable but also require continuous improvement. Therefore, the plan is to continue to promote the establishment of cybersecurity monitoring mechanisms by financial institutions or financial industry self-regulatory organizations of a certain scale or having a certain proportion of electronic transactions (based on importance), and to continuously analyze emerging attack methods used by hacker organizations and expand the coverage of cybersecurity monitoring and configuration baselines.

(14) Create Cloud-Ground Cybersecurity Alignment; Ensure Cybersecurity Standards are Kept

Financial institutions have laid a foundation with on-premise cybersecurity protection. However, the cloud environment and traditional on-premise architecture differ in terms of control responsibilities as well as technical

challenges. According to the cloud shared responsibility model, improper management of the respective security responsibilities of cloud service providers and financial institutions can easily cause management gaps and create spillover risks.

Since 2024, the FSC has worked to extend cybersecurity monitoring and configuration baselines to include cloud service environments. In March 2025, referencing the MITRE ATT&CK Cloud Matrix[52] and the CIS Benchmarks released by the Center for Internet Security (CIS) for public cloud infrastructure services (such as account management, static data storage, managed virtual machines, audit logs, serverless computing, secret and key management, and IaaS)[53], financial cloud cybersecurity monitoring and configuration baselines were provided for financial institutions to reference when planning to introduce cloud services. To respond to the rapid development of cloud services, the plan is to continuously expand the scope of efforts (to include, for example, container services, PaaS, etc.) to ensure consistent and high-level cybersecurity protection in cloud-ground alignment.

(15) Encourage Assessment of Monitoring and Protection Effectiveness

Cybersecurity monitoring and protection emphasize early detection and handling as well as creating a dense protection net. However, relying purely on a defensive mindset will inevitably lead to omissions. Therefore, the FSC continues to encourage financial institutions to adopt an attacker's mindset, periodically verifying the effectiveness of

[52] https://attack.mitre.org/matrices/enterprise/cloud/
[53] https://www.cisecurity.org/cis-benchmarks

cybersecurity monitoring and defense deployment through network attack methods such as DDoS offensive and defensive drills, red and blue team exercises, and breach and attack simulations.

6. Deploy Early to Address the Challenges of Emerging Technologies

(16) Employing Artificial Intelligence (AI): Enhancing Efficiency, Safeguarding Trust

The rapid development of the technology has accelerated the use of AI in financial institutions. Considering that the cybersecurity risks of AI systems intersect with those of traditional systems but are more complex and concealed, traditional cybersecurity policies cannot be directly applied. Rather, an AI-specific cybersecurity framework is required. Therefore, the plan references the established OWASP Generative AI Security Project[54] and MITRE's release of MITRE ATLAS (Adversarial Threat Landscape for AI Systems)[55] based on MITRE ATT&CK. Incorporating relevant security design and testing mechanisms as key points for subsequent study, the plan calls for the development of reference guidelines for AI system security protection and testing within the financial industry. This will guide the financial industry to include risk assessment or threat modeling for AI system design so as to cover traditional cyber threats and AI-specific attacks, introduce privacy-enhancing technologies that address specific scenarios, and appropriately conduct security-related testing, verification, and drills for AI systems so as to reduce exposure to AI threats.

[54] https://genai.owasp.org/
[55] https://atlas.mitre.org/

(17) Inventorying Cryptographic Assets and Assessing Posture, Migrating to Layout Post-Quantum Cryptography

Quantum computers have been shown to pose a severe threat to asymmetric encryption techniques. This will affect the encryption security of online transactions, electronic signatures, and identity verification. The US NIST released three documents addressing Post-Quantum Cryptography (PQC) algorithm standards[56] in March 2025.

To mitigate the risks caused by the development of quantum computing, the US FS-ISAC established a PQC working group and has released reports since 2023 concerning the need to inventory infrastructure encryption technologies, draft PQC readiness roadmaps, build crypto-agility, and address the effects of this technology on the payment card industry[57]. The FSC established a pilot group in July 2025, convening representative stakeholders and establishing a communication platform through F-ISAC to build consensus and draft PQC migration preparation items. This will involve progressively creating technology inventories to identify encryption technologies used in ICT (including network protocols, hardware equipment, and software packages), assessing their security levels and business risks (including, at a minimum, data confidentiality duration, business impact, business dependencies, ecosystem correlation, international alignment, and cryptographic vulnerability factors), and doing other groundwork (including, at a minimum, training technical personnel, surveying major suppliers, enhancing crypto-agility, and formulating system replacement procurement strategies). The aim is to develop reference

[56] https://csrc.nist.gov/projects/post-quantum-cryptography
[57] https://www.fsisac.com/knowledge/pqc

guidelines for financial industry PQC migration, providing a basis for the financial industry to establish PQC migration plans, and promoting, in a timely fashion, PQC migration within the financial industry based on the maturity of quantum computers and PQC development.

C. Collaborative Ecosystem Defense: Building Cross-Domain Joint Defense and Intelligent Intelligence Ecosystems

Strengthen the transparency and accountability of suppliers regarding cybersecurity, and enhance the maturation of cybersecurity along the supply chain through cross-industry joint defense collaboration, so as to increase the operational efficiency of cybersecurity joint defense efforts and the resilience of the overall financial ecosystem.

7. Enhance Supply Chain Cybersecurity to Fortify the Financial Ecosystem

(18) Develop Supplier Classification and Outsourcing Cybersecurity Responsibility Reference Templates

With the digital transformation and related developments in the financial ecosystem, the financial industry's reliance on third-party service providers and outsourcers has grown. Thus the supply chain is becoming increasingly diverse and complex. The plan addresses increased attacks on the supply chain by calling for classifying suppliers based on industry attributes, categorizing information systems accessed by suppliers, and triaging data sensitivity. The aim is to develop reference clauses for outsourcing contracts regarding cybersecurity responsibilities. This can include service level agreements (SLA), data protection responsibilities, time limits for reporting cybersecurity incidents, and cybersecurity

risk disclosure. Additionally, during the software security development phase, financial institutions are to require suppliers to provide proofs of security testing for their products or services and software bills of materials, and to cooperate with cybersecurity testing and drills. These measures are reference for financial institutions to help them improve cybersecurity management at their suppliers.

(19) Encourage Cybersecurity Intelligence Sharing and Collaboration with Key Suppliers

In addition to having F-ISAC continuing to obtain supplier anomaly information from intelligence sources like TWCERT/CC and industry cybersecurity alliances, and sharing supplier-related vulnerability information along with attack methods and defense strategies, financial institutions are encouraged to establish supply chain risk assessment mechanisms of their own. They can do so by cooperating with upstream and downstream partners such as key suppliers, third-party service providers, and system integrators to share threat and protection information, strengthen controls, and conduct joint cybersecurity exercises, thereby reducing the cybersecurity risk along the entire supply chain.

8. Strengthen Cybersecurity Intelligence Analysis and Collaborative Defense

(20) Strengthen Cybersecurity Intelligence Correlation Analysis and Intelligence Sharing Momentum

Since establishing F-ISAC at the end of 2017 to promote financial cybersecurity joint defense, the FSC has established horizontal links among financial institutions. Additionally, a cybersecurity intelligence correlation analysis platform was set up at the end of 2022 to provide automated intelligence

interfacing and intelligence-sharing reward mechanisms. To increase the usability and breadth of intelligence interfacing, the plan is to strengthen existing automated (API) sharing mechanisms, allowing members to obtain intelligence based on demand types. There are also plans to enhance intelligence-sharing reward measures to encourage members to collect and share ecosystem-related exposure intelligence.

(21) Establish Financial Cybersecurity Vulnerability Notification and Response Channels

To reduce the external exposure of financial institutions, starting from 2025, the FSC has been simulating a hacker's perspective to determine whether unpatched vulnerabilities, insecure encryption mechanisms, or incorrect configuration settings are present in the internet services of financial operators. Detection results are then converted into cybersecurity intelligence and passed on to financial institutions by F-ISAC for them to address. Aside from continuing with these operations, F-ISAC plans to establish financial cybersecurity vulnerability notification and response channels that will expand the sources of financial cybersecurity vulnerability notifications. After an initial assessment, these will then be referred to financial institutions for handling, reducing the risk of cyberattacks.

(22) Enhance Effectiveness of Collaboration between Financial Institution SOCs and Joint Defense SOCs

The FSC continues to encourage financial institutions to build SOCs and supervises F-ISAC's efforts to create a Joint Defense SOC. To perform more efficient correlation analysis on incident tickets returned by participating financial institutions, F-ISAC is tasked with guiding financial

institution SOCs to introduce cybersecurity monitoring and configuration baselines, enhancing the timeliness and effectiveness of the Joint Defense SOC's correlation analysis of incident tickets that have been put into the system. To further increase the analytical value of the Joint Defense SOC for incident tickets, the plan introduces automated analysis mechanisms to improve the extraction and comparison of key information (such as attack methods, impact scope, attack chain position) in incident tickets. Combined with threat intelligence databases for correlation analysis, and by establishing incident ticket content classification and priority standards, the SOC's precision and timeliness in incident judgment, trend mastery, and early warning notification will be improved, thereby providing financial institutions with more efficient analysis results.

(23) Strengthen International Financial Cybersecurity Cooperation

Since its establishment, F-ISAC has successively joined the US FS-ISAC as a member, attended the EU FI-ISAC annual meeting, signed MOUs with Japan's F-ISAC and Thailand's TB-CERT, and became a member of the Forum of Incident Response and Security Teams (FIRST) as well as the Asia Pacific Computer Emergency Response Team (APCERT). To continually strengthen the sharing of cybersecurity threat intelligence among international partners, the plan calls for organizing regular transnational online exchanges to share information on recent attacks, trends, and defense strategies used in Taiwan. It also involves periodically providing English-language versions of Taiwan's threat analysis reports and overall threat posture reports, deepening exchanges with international partners, enhancing

international visibility, and strengthening the early warning and response benefits of cross-border incidents.

D. Robust Resilience: Ensuring Critical Service Continuity and Rapid Recovery

Ensure uninterrupted critical financial services through drills, backups, and risk layering, thus achieving sustainable operation and rapid recovery.

9. Conduct Cybersecurity Offensive and Defensive Drills to Enhance Incident Response Capabilities

(24) Conduct DDoS, Network Offensive/Defensive, or Other Cybersecurity Drills for Financial Institutions

Traditional cybersecurity defense methods tend to focus on the defensive side, often falling into a passive stance wherein hackers control the initiative. Therefore, to strengthen the defense energy against hacker attacks, the FSC introduces the attack and defense methodology released by MITRE (MITRE ATT&CK & ENGAGE). In line with the *Financial Cybersecutity Action Plan* promotion measures, the FSC conducts financial cybersecurity offensive and defensive drills to improve frontline defense capabilities.

(25) Hold Specialized Financial Cybersecurity Training Classes

In addition to continuing the aforementioned offensive and defensive drills, considering the differences in the scale of financial institutions and cybersecurity human resources, to expand training on defense awareness and skills, the plan calls for collaboration with training institutions to expand participation via specialized training classes.

(26) Conduct Major Cybersecurity Incident Response Scenario Exercises

In addition to continuing offensive/defensive drills and training classes, to verify the operability of command systems during major cybersecurity incidents and expand the breadth and depth of drill scenarios, response scenario drills such as ransomware, supply chain attacks, and cloud service provider outages are planned. These will appropriately verify the notification, coordination, and support mechanisms among financial institutions, financial holding group computer cybersecurity incident response teams, financial industry self-regulatory organizations or association cybersecurity response support teams, and the F-ISAC joint defense system.

10. Reinforce Multi-Layered Backup Mechanisms to Ensure Availability of Critical Financial Services

(27) Encourage Adoption of International Business Continuity Management Standards and Acquisition of Relevant Certifications

To provide a common language and complete framework for Business Continuity Management (BCM) internationally, the International Organization for Standardization established international standards on BCM. The FSC encourages financial institutions to adopt these standards as well as best practices. It encourages verification of compliance with various requirements from internal sources, regulations, and customers through independent third-party institutions, using this to communicate preparedness for shocks to stakeholders.

(28) Respond to Composite Disaster Scenarios, Establish Multi-Layered Backup Mechanisms for Critical Services

When releasing the *Financial Cybersecurity Action Plan*

2.0, the FSC kept in mind that the preservation of financial core business data is critical to ensuring property rights in financial institutions. To respond to such issues as major cybersecurity incidents, natural disasters, and geopolitical shifts, in addition to existing local and remote backup and recovery mechanisms, strengthening financial institution critical data preservation mechanisms (such as third-site or cloud backup) was named a priority. To continually improve disaster recovery capabilities and business continuity resilience, the plan advocates continuing to advance multi-layered backup architecture for critical financial services. Based on a Business Impact Analysis (BIA), the minimum recovery needs for various backup scenarios are assessed, and Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) are set as the baseline for backup design and resource allocation. Considering cross-region resource scheduling and command operations when actual disasters occur, regular testing and drill verification are conducted to ensure switching operations can be performed if any layer fails, prioritizing the recovery of critical financial services.

(29) Assess and Establish Operational Continuity Capacity and Backup Collaboration Mechanisms for the Critical Financial Service Ecosystem

Considering that financial services rely heavily on external suppliers and ecosystem partners (such as core system vendors, telecom operators, payment processors, API interface objects, etc.), financial institutions should continually assess whether the disaster recovery and backup capabilities of key supply chain partners are sufficient to support critical financial services. They should establish relevant backup collaboration mechanisms or draft alternative

measures, incorporating them into backup and drill planning.

V. Promotion and Evaluation

A. **Public-Private Partnership:** The public sector, financial industry self-regulatory organizations, and the various financial industry associations will adopt related regulatory rules and standards, cultivate cybersecurity personnel, and coordinate on cyber monitoring and response, in order to help financial institutions improve their cyber defense capabilities.

B. **Differentiated Regulatory Treatment:** Depending on the particular characteristics of different lines of business, the size of different financial institutions, and operational risks, the FSC will adopt appropriately graded cybersecurity standards that pay balanced attention to financial institutions' actual cyber defense needs as well as the feasibility of implementation.

C. **Resource Sharing:** Continue promoting cyber intelligence sharing and cooperation, establish a financial cyber incident response and monitoring system, implement cybersecurity joint defense, encourage financial industry self-regulatory organizations (or financial industry associations) to establish a cybersecurity incident response team, and use resource sharing and cooperation to strengthen financial cyber defense capabilities.

D. **Compliance Incentives:** The competent authority can use supervisory measures (e.g. including cybersecurity risk factors among the matters it takes into consideration when: deciding whether to approve applications to conduct a new line of business; determining regulatory capital charges; calculating premium rates for deposit insurance or the Taiwan Insurance Guaranty Fund) to guide financial institutions to actively implement cybersecurity measures.

E. **International Cooperation:** Obtain international financial cyber intelligence by strengthening exchanges and cooperation

or signing MOUs with financial cybersecurity authorities in other countries, and engage with international cybersecurity organizations in a joint effort to strengthen cyber defenses.

After the release of this blueprint, the FSC will convene various bureaus, relevant financial industry self-regulatory organizations, and industry associations to jointly define promotion indicators and execution schedules for each item. Starting from 2026, execution status will be reviewed quarterly, while promotion strategies, execution measures, and various promotion indicators will be revised on a rolling basis.

VI. Expected Benefits

A. **Policy:** Adopt a dual-track system, promoting both standardization through industry regulations and optimization through best practices in parallel. Establish short, medium, and long-term goals to gradually reduce the burden of compliance on the financial industry. Lead the maturation of cybersecurity governance and resilience at the management level of financial institutions to provide better support for financial service innovation and the secure introduction of AI applications.

B. **Management:** Through promoting the financial industry to strengthen software security, supply chain security management, and collaboration mechanisms, enhance cross-industry protection and recovery capabilities, reduce the effect of supplier cybersecurity incidents on the financial industry, and guarantee financial stability.

C. **Technical Aspect:** By encouraging the financial industry to gradually introduce Zero Trust Architecture, establish multi-layered backups and expand the scope of drills, enhance financial institutions' implementation of tactics, techniques, and procedures, and reduce the mean time to recover (MTTR) for

major incidents.

D. **Internationally:** Through a continual improvement of the operational resilience of domestic financial institutions and by enhancing cooperation with international financial cybersecurity organizations, improve the international trust rating for Taiwan's financial cybersecurity efforts, facilitating cross-border cooperation and foreign investment by financial institutions.

VII. Outlook

Cybersecurity threats will not diminish even with the improvement of financial institution defense capabilities; rather, they will become more complex due to continuing technological innovation. Therefore, the financial system must shift from a mindset of prevention to a more resilience-oriented one of seeking a rapid response and rapid recovery.

The four-axis framework proposed in this blueprint combines international supervisory trends, Taiwan's practical status, and the direction of technological development. By strengthening the accountability chain of senior governance, introducing forward-looking technical protections (such as shift-left security, zero trust architecture, and AI/PQC deployment), expanding the collaborative defense of the entire supply chain, and conducting multi-layered backups and routine drills, the goal is to establish a resilience governance model in the financial industry that is: *Executable*, *Measurable*, *Improvable*, and *Internationally Aligned*. The ultimate aim is to build a *Secure*, *Trusted*, and *Sustainably Innovative* financial ecosystem in Taiwan.