BANGKO SENTRAL NG PILIPINAS

FSCRP

FINANCIAL SERVICES CYBER RESILIENCE PLAN

2024-2029

FORTIFYING CYBER FRONTIER FOR
BSP-SUPERVISED FINANCIAL INSTITUTIONS

www.bsp.gov.ph

BANGKO SENTRAL
NG PILIPINAS

TECHNOLOGY RISK AND INNOVATION SUPERVISION DEPARTMENT
2024

GOVERNOR'S MESSAGE

The 2024-2029 Financial Services Cyber Resilience Plan (FSCRP) is an important step in the financial services industry's cybersecurity journey. It supports the BSP's mission to fortify the security posture of the financial system and is aligned with the country's National Cybersecurity Plan 2028 (NCSP 2028).

In an era where digital transformation is reshaping the financial landscape, robust cybersecurity measures has never been more critical. The FSCRP is our proactive response to the growing complexities of cyber threats. It embodies our commitment to safeguarding the integrity and stability of the financial system and the trust in the system.

Developed through the collaborative effort of relevant stakeholders, the FSCRP covers high-level goals and strategic initiatives to respond to evolving threats and address systemic cyber risks. It also outlines industrywide measures to enhance information sharing and collaboration, strengthen cybersecurity culture and awareness, and promote best practices and standards across various cybersecurity domains.

As we embark on this journey, I urge all stakeholders to embrace this plan as a commitment to building trust, reliability and security in financial services for every Filipino.

Mabuhay!

Eli M. Remolona, Jr.
Governor
Bangko Sentral ng Pilipinas

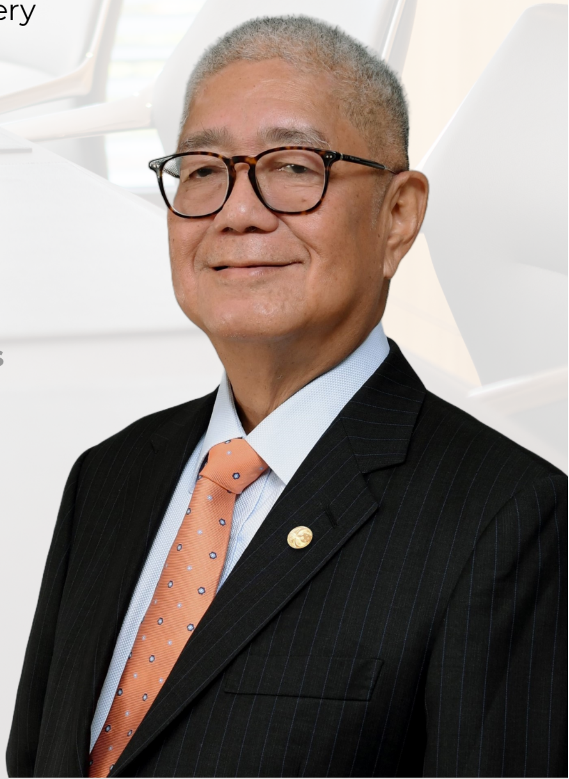


TABLE OF CONTENTS

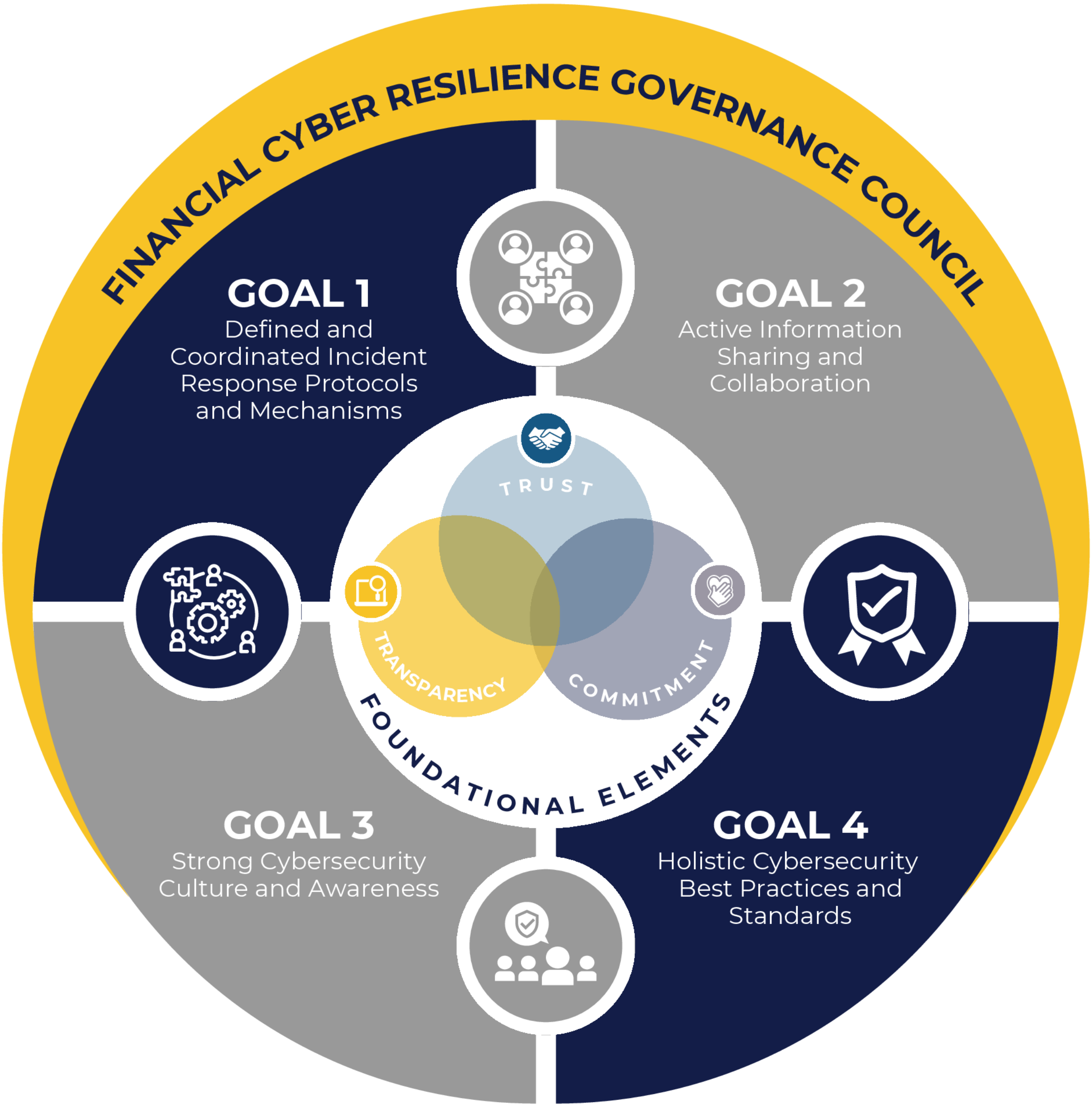
VISION *and* MISSION

VISION

A safe, secure, and resilient financial system that fosters strong cybersecurity culture, governance, and collaboration to advance digital financial inclusion and consumer protection.

MISSION

To continually enhance the industry's cybersecurity capabilities and maturity, strengthen collaboration, and pursue holistic reforms to proactively address existing and emerging cyberthreat concerns, and preserve public trust and confidence in the digital financial system.


FINANCIAL CYBER RESILIENCE GOVERNANCE COUNCIL
GOAL 1
Defined and Coordinated Incident Response Protocols and Mechanisms
GOAL 2
Active Information Sharing and Collaboration
GOAL 3
Strong Cybersecurity Culture and Awareness
GOAL 4
Holistic Cybersecurity Best Practices and Standards
TRUST
TRANSPARENCY
COMMITMENT
FOUNDATIONAL ELEMENTS

FSCRP STRATEGY MAP

EXECUTIVE SUMMARY

The Bangko Sentral ng Pilipinas (BSP) considers cybersecurity as a key strategic enabler in fostering digital innovation in the financial services industry and more importantly, in maintaining financial stability. In 2015, the BSP established the Cybersecurity Roadmap to institutionalize cyber resilience covering three main areas on capacity building, collaborative engagements, and continuing policy framework and supervisory enhancements. Since the establishment of the BSP's Cybersecurity Roadmap, cybersecurity policies and reforms aimed at greater cyber resilience in the financial system have been implemented.

With the growing cyberthreat landscape and a clear mandate to serve as the Lead Computer Emergency Response Team (CERT) of the Banking Sector[1], which is considered a Critical Information Infrastructure (CII) in the country, the BSP endeavors to concretize its cybersecurity plans and objectives through the 2024-2029 Financial Services Cyber Resilience Plan (FSCRP).

The FSCRP shall serve as the primary framework covering the high-level goals and strategies that aim to deepen the industry's overall cyber resilience and maturity. The FSCRP covers four high-level goals or strategic outcomes:

Goal 1 - Defined and coordinated incident response protocols and mechanisms
Goal 2 - Active information sharing and collaboration
Goal 3 - Strong cybersecurity culture and awareness
Goal 4 - Holistic cybersecurity best practices and standards

High-Level Goals	Strategy Summary
Goal 1: Defined and coordinated incident response protocols and mechanisms	This covers strategies to sharpen the industry's capabilities to proactively respond to and recover from major cyber incidents. Priority actions under this goal are: • **D1:** Establish baseline industry incident response plan • **D2:** Develop scenario-based incident response playbooks • **D3:** Conduct progressive industry-wide cyber testing exercise regime • **D4:** Explore setting up of an industry Security Operations Center (SOC)
Goal 2: Active information sharing and collaboration	This encompasses strategies to institutionalize and expand sharing of timely and actionable cyberthreat intelligence across the financial community, including coordination and collaboration with other industry stakeholders and the National CERT (CERT-PH). Priority actions under this goal are: • **A1:** Expand and further enhance Bankers Association of the Philippines Cybersecurity Incident Database (BAPCID) as an industry sharing platform • **A2:** Strengthen and forge strategic partnerships in domestic and international fora • **A3:** Support the enactment of cyber-related legislative initiatives (e.g., Anti-Financial Account Scamming Act, Liberalization of Secrecy of Deposits, etc.)
Goal 3: Strong cybersecurity culture and awareness	This goal covers strategies to instill strong cybersecurity culture and enhance cybersecurity skills and capabilities in the financial services industry. Key priority actions include: • **S1:** Develop and implement cyber education program for BSFI Board and Senior Management • **S2:** Regularly conduct Chief Information Security Officer (CISO)/cyber forum and Annual Cybersecurity Summit • **S3:** Conduct cybersecurity roadshows for small and medium-sized financial institutions (FIs) • **S4:** Pursue holistic programs on cybersecurity skills and talent development • **S5:** Mainstream cyber education and awareness programs for financial clients
Goal 4: Holistic cybersecurity best practices and standards	This goal contains strategies to promote cybersecurity best practices and standards across cybersecurity domains. Priority actions under this goal are: • **H1:** Complete policy reforms on digital security controls, Application Programming Interface (API) security, Cybersecurity Maturity Model (CMM) framework, and supply chain risk management • **H2:** Explore establishment of an Industry Cyber Innovation/Research Hub • **H3:** Conduct benchmarking exercises on cyber capabilities

To ensure smooth plan implementation, the FSCRP shall be assessed, at least quarterly, to adjust priority actions vis-à-vis developments in the cyberthreat landscape. Metrics shall also be developed to determine the level of achievement of each key goal as well as evaluate the industry's overall cyber resilience posture. To ensure strong commitment and support, the FSCRP implementation and progress shall be overseen by the Financial Cyber Resilience Governance Council, composed of board and senior level officials from relevant industry associations, select systemically important BSP-Supervised Financial Institutions (BSFIs) and senior management of the BSP.

The FSCRP shall apply to all BSFIs, relevant financial market infrastructures (FMIs) within the BSP's supervisory authority, cybersecurity organizations, and private-sector participants that provide critical IT and information security infrastructure/services to the BSFIs. Said plan shall be aligned to the extent possible with the NCSP 2028 as well as existing regulations and policy issuances of the BSP.

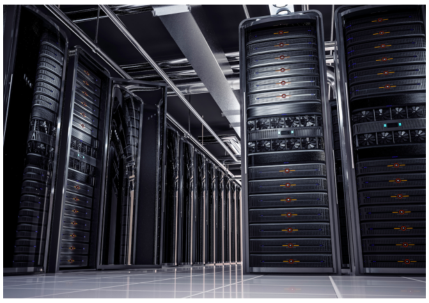
SCOPE AND APPLICABILITY

PLAN LINKAGES & CONSIDERATIONS

Given the multi-dimensional aspect of cybersecurity, the plan takes into consideration the BSP's ongoing work on financial inclusion, financial consumer protection, open finance, anti-money laundering, operational resilience, and enhanced work on systemic risk oversight and resolution.

Digital technologies serve as a critical enabler for financial inclusion to enhance market reach and expand delivery channels. In the 2022-2028 National Strategy for Financial Inclusion (NSFI), digital financial inclusion is identified as one of the strategic goals to facilitate delivery of innovative and cost-effective financial services to low-income mass market and small enterprises. Alongside growing digitalization of financial products and services, cyber criminals are increasingly shifting their tactics and scams against vulnerable financial consumers. This necessitates BSFIs to incorporate cybersecurity awareness and education for their clients to avoid being victims of scams and cyber fraud. To entice the financially excluded market or business to avail of digital financial services, it is imperative to incorporate sound technology risk management and cyber resilience mechanisms in the underlying digital financial infrastructure. The FSCRP supports digital financial inclusion and financial consumer protection through priority initiatives under Goals 3 and 4 on "strong cybersecurity culture and awareness" and "holistic cybersecurity best practices and standards," respectively.

In 2021, the BSP developed the Open Finance (OF) Roadmap, which sets long-range plans to mainstream open finance in the country. The OF Framework under BSP Circular No. 1122 promotes consent-driven data portability, interoperability, and collaborative partnerships among BSFIs and fintech providers to develop and offer innovative financial products and services. With open API as the core technology supporting OF, cybersecurity, along with usability and standardization, are crucial elements for OF's success. The FSCRP supports the BSP's open finance initiative through Goal 4 on "holistic cybersecurity best practices and standards," which identifies API security as a priority policy reform.



Cyberthreats and attacks are closely linked to money laundering as proceeds of cyber fraud and scams are considered as money laundering offenses. In particular, money mules[2] is commonly employed to monetize cyber attacks. Currently, there are legal hurdles that constrain the conduct of expedient and in-depth cyber investigation (e.g., lack of legal anchor to hold or freeze accounts, limitations due to strict bank secrecy laws, etc.). As such, support for key legislative initiatives as well as the ongoing close coordination with supervisors involved in anti-money laundering (AML) activities or procedures are included under Goal 2 on "active information sharing and collaboration" of the FSCRP in order to close the gaps.

Cyberthreats and attacks launched against financial institutions, particularly critical financial infrastructure, can cause significant disruptions leading to broader implications for financial stability (Financial Stability Board [FSB], 2020). Understanding financial stability risks caused by a cyber event is crucial because additional capital and liquidity may not reduce the impact of a cyber risk in the same way that they mitigate financial losses (Federal Reserve, 2022). The Federal Reserve (2022) stated that while capital and liquidity can provide the financial resources needed to respond to a cyber incident, they may not hasten the process of restoring systems, data, or confidence in the industry's integrity.

With interconnected IT systems among multiple financial institutions, a cyber attack at a single bank, for example, might impede the bank's capacity to transfer payments, affecting the liquidity and operations of other banks. Finally, when financial products and services are provided by a small number of fintech players, cyber risk can increase market concentration in the banking system.

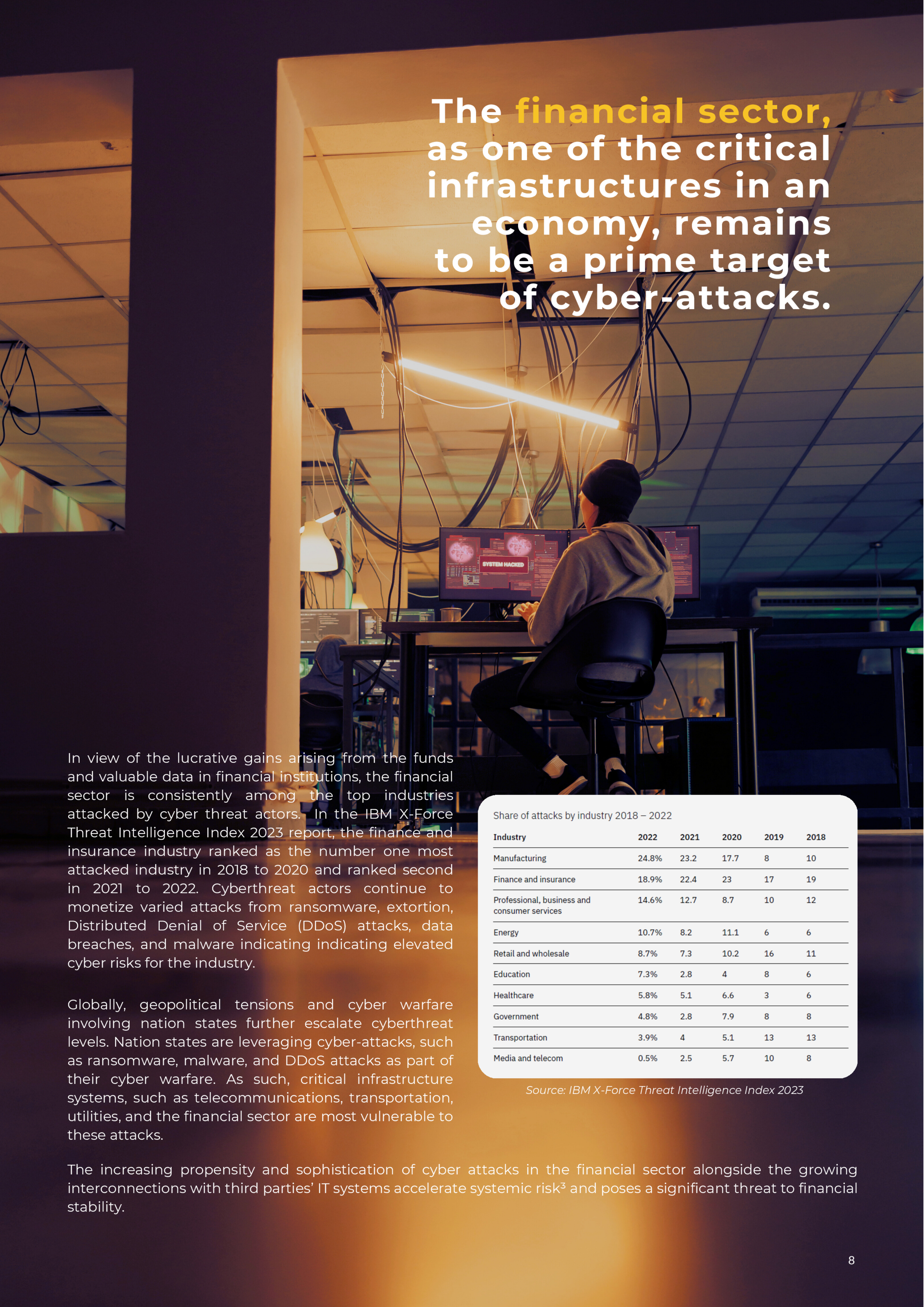
It is becoming more crucial for BSFIs to swiftly resume critical operations and minimize operational, financial, legal, reputational, and other material risks arising from these systemic disruptions. Hence, effective cyber resilience mechanisms must be in place and integrated into the BSFIs' business continuity management and operational resilience programs. The approach to tackle these concerns is further elucidated under Goal 4 of the FSCRP on "holistic cybersecurity best practices and standards".

CYBERTHREAT OVERVIEW

FINANCIAL SERVICES

The business models for financial services are radically shifting from traditional to digital-centric. The shift became even more pronounced during the COVID-19 pandemic as more Filipinos avail digital payment and financial services. The increased consumer demand for digital products and services along with the adoption of remote work arrangements compelled financial institutions to accelerate their digital transformation initiatives.

Fast-paced innovations in artificial intelligence (AI), blockchain, cloud computing, big data, and other emerging technologies as applied to financial services add complexity and widen the attack surface and methodologies. These developments and the increasing role of technology in driving the strategies and mission-critical services of financial institutions highlight the need to reinforce cybersecurity and resilience for the financial services industry.



The financial sector, as one of the critical infrastructures in an economy, remains to be a prime target of cyber-attacks.

In view of the lucrative gains arising from the funds and valuable data in financial institutions, the financial sector is consistently among the top industries attacked by cyber threat actors. In the IBM X-Force Threat Intelligence Index 2023 report, the finance and insurance industry ranked as the number one most attacked industry in 2018 to 2020 and ranked second in 2021 to 2022. Cyberthreat actors continue to monetize varied attacks from ransomware, extortion, Distributed Denial of Service (DDoS) attacks, data breaches, and malware indicating indicating elevated cyber risks for the industry.

Globally, geopolitical tensions and cyber warfare involving nation states further escalate cyberthreat levels. Nation states are leveraging cyber-attacks, such as ransomware, malware, and DDoS attacks as part of their cyber warfare. As such, critical infrastructure systems, such as telecommunications, transportation, utilities, and the financial sector are most vulnerable to these attacks.

Share of attacks by industry 2018 – 2022

Industry	2022	2021	2020	2019	2018
Manufacturing	24.8%	23.2	17.7	8	10
Finance and insurance	18.9%	22.4	23	17	19
Professional, business and consumer services	14.6%	12.7	8.7	10	12
Energy	10.7%	8.2	11.1	6	6
Retail and wholesale	8.7%	7.3	10.2	16	11
Education	7.3%	2.8	4	8	6
Healthcare	5.8%	5.1	6.6	3	6
Government	4.8%	2.8	7.9	8	8
Transportation	3.9%	4	5.1	13	13
Media and telecom	0.5%	2.5	5.7	10	8

Source: IBM X-Force Threat Intelligence Index 2023

The increasing propensity and sophistication of cyber attacks in the financial sector alongside the growing interconnections with third parties' IT systems accelerate systemic risk[3] and poses a significant threat to financial stability.

PHISHING

CONTINUES TO BE A TOP ACCESS VECTOR FOR CYBER ATTACKS

Cyber fraud and attacks continue to evolve in the financial services industry and remain an area of concern especially in line with the digital acceleration in recent years. Based on the cyberthreat reports submitted by BSFIs, 59.48% of the cyber fraud losses in 2023, emanates from account takeover, identity theft, and phishing. This represents a 212% jump from 2022 cyber fraud losses. This shows that cyber threat actors are predominantly targeting human vulnerabilities in perpetrating cyber schemes.

There are also various ways and scams where financial consumers may be defrauded in giving out personal and sensitive information. Simple schemes like filling out forms or sharing personal information to a person or entity that mishandled data may be a starting point for an attack. Likewise, compromised emails, social media platforms, and vishing are largely, utilized indicating that threat actors are willing to spend time and resources in gathering information and executing an attack.

> Cyberthreats and incidents are rising with scores of phishing, online fraud, API attacks, DDoS, and other malware attacks targeting supervised institutions, their third-party networks, and their clients. Most attacks underpin the inherent vulnerability of the "human" component in cybersecurity; hence, there's a need to ramp up cyber awareness and education programs as more people are migrating to digital financial products and services. – *TRISD Staff*

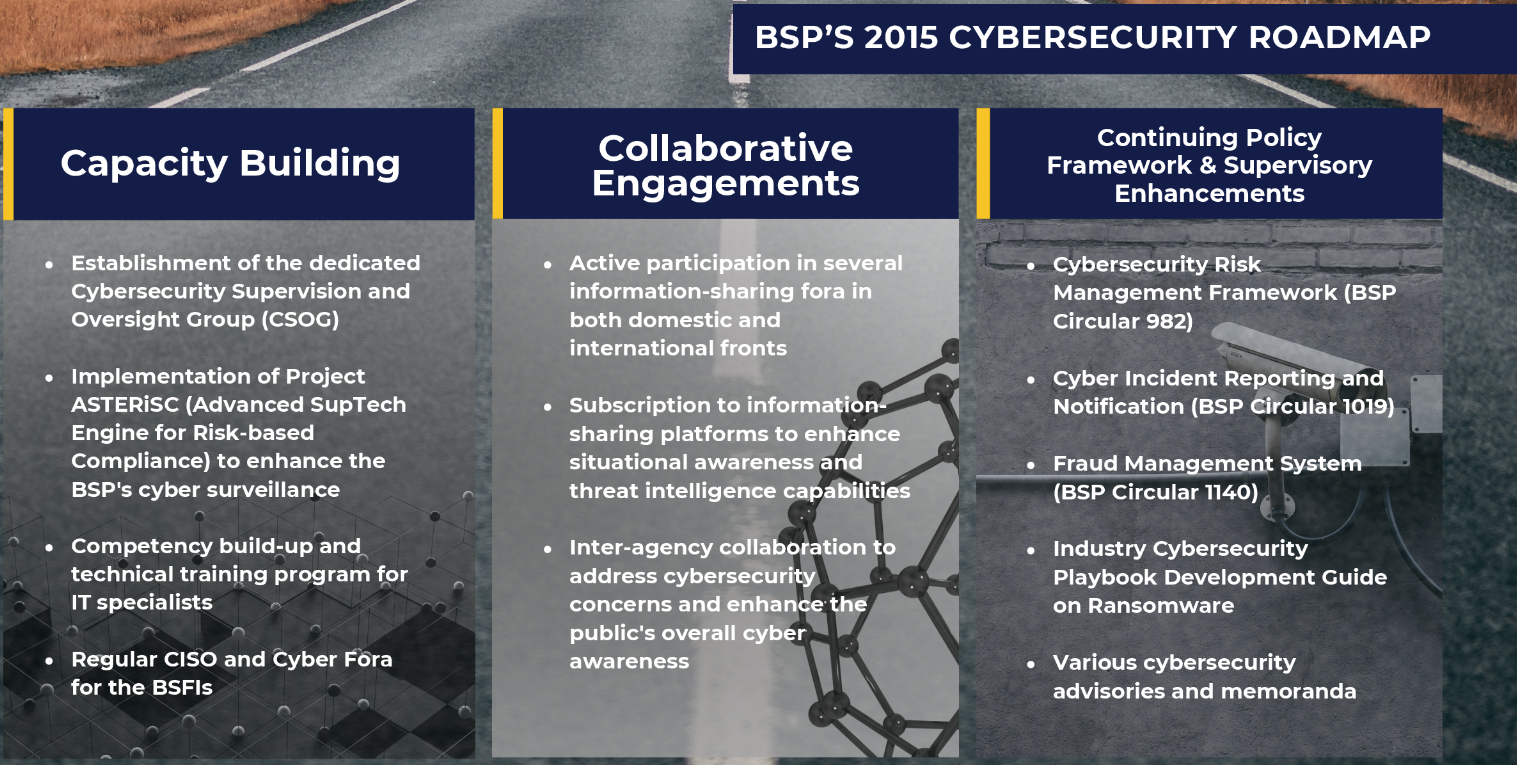
Cyberthreat actors are innovating their cyber attacks by leveraging emerging technologies. For instance, generative AI are being utilized to craft more convincing phishing emails, conduct identity takeover through “deep fake” technology, and create destructive malware variants. The rise of internet of things (IoT) devices also poses heightened security risks, which can have real-world repercussions. According to an article by CNBC, there are around 17 billion IoT devices in the world, from printers to garage door openers, each one packed with software that can be easily hacked[4]. Another area of concern relates to the cybersecurity implications of quantum computing, a rapidly emerging technology that harnesses the laws of quantum mechanics to solve problems too complex for classical computers.[5] With its exponential processing capabilities, cyberthreats include data breaches of sensitive health and financial data, challenges to the integrity of digital assets, and breaking the fundamental cryptography underpinning cryptocurrencies.[6]

The above trends correspond to a report by the World Economic Forum (WEF) highlighting geopolitical instability, rapidly maturing and emerging technologies, and emerging threats as among the significant challenges confronting cyber and business leaders globally. This is further complemented by the WEF Global Cybersecurity Outlook 2024 Report citing the additional constraints brought about by emerging technologies, particularly generative AI, in achieving cyber resilience.

EMERGING TECHNOLOGIES
ARE RAPIDLY CHANGING THE
CYBERTHREAT ECOSYSTEM

CYBERSECURITY AS A KEY BSP SUPERVISORY PRIORITY

As cybersecurity supports core mandates on financial stability, financial inclusion, and digital transformation, the BSP has been steadfastly working to institutionalize cyber resilience in the financial services industry. This legwork is embodied in the BSP's 2015 Cybersecurity Roadmap covering three key areas on capacity building, collaborative engagements and continuing policy framework, and supervisory enhancements. In implementing the roadmap, the BSP is actively fostering a responsive regulatory landscape, forging collaborative partnerships, and fortifying surveillance capabilities. *Figure 1* outlines some of the major initiatives under each of the three areas since 2015.



BSP'S 2015 CYBERSECURITY ROADMAP

Capacity Building

- Establishment of the dedicated Cybersecurity Supervision and Oversight Group (CSOG)
- Implementation of Project ASTERiSC (Advanced SupTech Engine for Risk-based Compliance) to enhance the BSP's cyber surveillance
- Competency build-up and technical training program for IT specialists
- Regular CISO and Cyber Fora for the BSFIs

Collaborative Engagements

- Active participation in several information-sharing fora in both domestic and international fronts
- Subscription to information-sharing platforms to enhance situational awareness and threat intelligence capabilities
- Inter-agency collaboration to address cybersecurity concerns and enhance the public's overall cyber awareness

Continuing Policy Framework & Supervisory Enhancements

- Cybersecurity Risk Management Framework (BSP Circular 982)
- Cyber Incident Reporting and Notification (BSP Circular 1019)
- Fraud Management System (BSP Circular 1140)
- Industry Cybersecurity Playbook Development Guide on Ransomware
- Various cybersecurity advisories and memoranda

Figure 1. BSP's 2015 Cybersecurity Roadmap

FOSTERING A RESPONSIVE REGULATORY LANDSCAPE

In response to the evolving digital and cyberthreat landscape surrounding BSFIs, the BSP has been actively promoting sound risk management principles to be adopted by BSP-supervised financial institutions (BSFIs) covering various facets of ICT and cybersecurity.

Since 2013, the BSP issued several regulations aimed at mitigating the effects of technology and cyber-related risks on financial institutions (*major cyber-related frameworks shown in Figure 2*). These regulations address various facets of technology, such as social media risk management, business continuity management, and multi-factor authentication, among others. Recent issuances include specific guidance on addressing phishing attacks against retail electronic payments and financial services (EPFS), API security as well as various threat intelligence on ransomware, and other forms of malware threats.

FRAMEWORKS

BSP CYBERSECURITY POLICY FRAMEWORKS

IT Risk Management Framework
BSP Circular 808 | 22 August 2013
Serves as the foundational framework for ITRM of BSFIs. This covers IT Governance, risk management, and controls implementation on various areas, namely, IT operations, information security, development and acquisition, IT outsourcing and vendor management, disaster recovery, and IT audit.

Cybersecurity Risk Management Framework
BSP Circular 982 | 09 November 2017
Presents a holistic framework on information security. The Circular also encompasses key elements of cyber resilience, such as participation in information sharing and collaboration fora, enhancing situational awareness capabilities as well as adoption of advanced cybersecurity controls, and countermeasures.

Cyber Incident Reporting and Notification
BSP Circular 1019 | 31 October 2018
Tightens the reporting regime of BSFIs with respect to cyber-related incidents and operational disruptions, from ten (10) calendar days to within two (2) hours from discovery of the incident, enabling more proactive cyber defense and response.

Fraud Management Framework
BSP Circular 1140 | 24 March 2022
Mandates the adoption of robust and real-time fraud management system backed by reinforced cyber awareness programs.

Figure 2. BSP Cybersecurity Policy Frameworks

FORGING COLLABORATIVE PARTNERSHIPS

With the fast-paced and systemic nature of cyber threats and attacks, collaboration among multiple stakeholders, fellow regulators, industry associations, law enforcement, and other government agencies is vital to strengthen cyber defenses and security posture. At present, the BSP is a party to several domestic and international information-sharing fora that delve on various topics, including technology risk management, innovation, payment systems, and cybersecurity (*Figure 3*). The BSP also closely coordinates with its counterparts in other jurisdictions for benchmarking and knowledge exchange. Moreover, the BSP has institutionalized membership in a national multi-sectoral coordinating agency for purposes of setting a better handle of the cyber posture of the financial system.

BSP COLLABORATIVE PARTNERSHIPS

Joint Anti-Bank Robbery Action and Cybercrime Coordinating Committee (JABRACCC). The BSP is part of the JABRACCC, which provides a mechanism for unified response and integrating efforts to enhance cybersecurity and safety of the banking system. Established in 2004, JABRACCC is a consortium among the Philippine National Police (PNP), Bankers Association of the Philippines (BAP), the Bank Security Management Association (BSMA), and other government agencies and private banking institutions.

Information Security Officers Group (ISOG). To encourage collaborative efforts and information sharing among the key players in the financial industry, the Information Security Officers' Group (ISOG) composed of Information Security Officers was established in 2014. The primary objective of ISOG is geared toward capacity building and development of preventive measures to combat cybercrime particularly those targeting financial institutions. The BSP played a key role in the realization of this endeavor by providing the necessary support and guidance for the industry players.

Joint Cyber Security Working Group (JCSWG) organized by the US Department of Justice – FBI Legat Manila. The JCSWG was established in August 2016 by the Office of the Legal Attache in Manila (LEGAT), partnering with the U.S. Department of State, and Philippine Government counterparts and private sector companies, both U.S. and Philippine-based, to promote intelligence sharing on cybersecurity. JCSWG is composed of over 300 individuals, including representatives from the Anti-Money Laundering Council, Bangko Sentral ng Pilipinas, National Bureau of Investigation – Cybercrime Division, and the Philippine National Police – Anti-Cybercrime Group, among others.

Bankers Association of the Philippines (BAP) Cybersecurity Committee. Formed in February 2017, the Committee serves as a forum to share cyber threat intelligence and information as part of early warning system, share best practices, and recommend enhancements in IT and cyber-related policies to better prevent, respond, and manage emerging cyber-threat concerns. The BSP is an advisory member of this Committee.

National Cybersecurity Inter-Agency Committee (NCIAC). The NCIAC serves as the lead for interagency body established for policy coordination among concerned agencies. Per Executive Order (EO) 95, s. 2019, the BSP Governor is a member of the NCIAC.

International IT Supervisory Group (ITSG). The ITSG is an independent and cooperative international working group for prudential IT Supervisors, whose objective is to actively support and encourage an effective international IT supervisory cooperation. ITSG consists of technology risk specialists and information security professionals from twenty (20) supervisory authorities in Europe, America, Asia, and Australia. The Philippines, through BSP-TRISD, attained its full membership status in 2017.

ASEAN CRISP Digital Technology Network (DTN). The BSP is a member of DTN as part of the ASEAN Cybersecurity Resilience and Information Sharing Platform (CRISP). The DTN is a network for ASEAN Cybersecurity and IT experts/supervisors with purpose of discussing and sharing cybersecurity related practices, policy recommendations, and mitigating solutions for the mutual benefits of ASEAN member countries. The CRISP is envisioned as a prelude to greater cooperation and coordination among ASEAN countries in building cybersecurity capabilities allowing better preventive and mitigating controls.

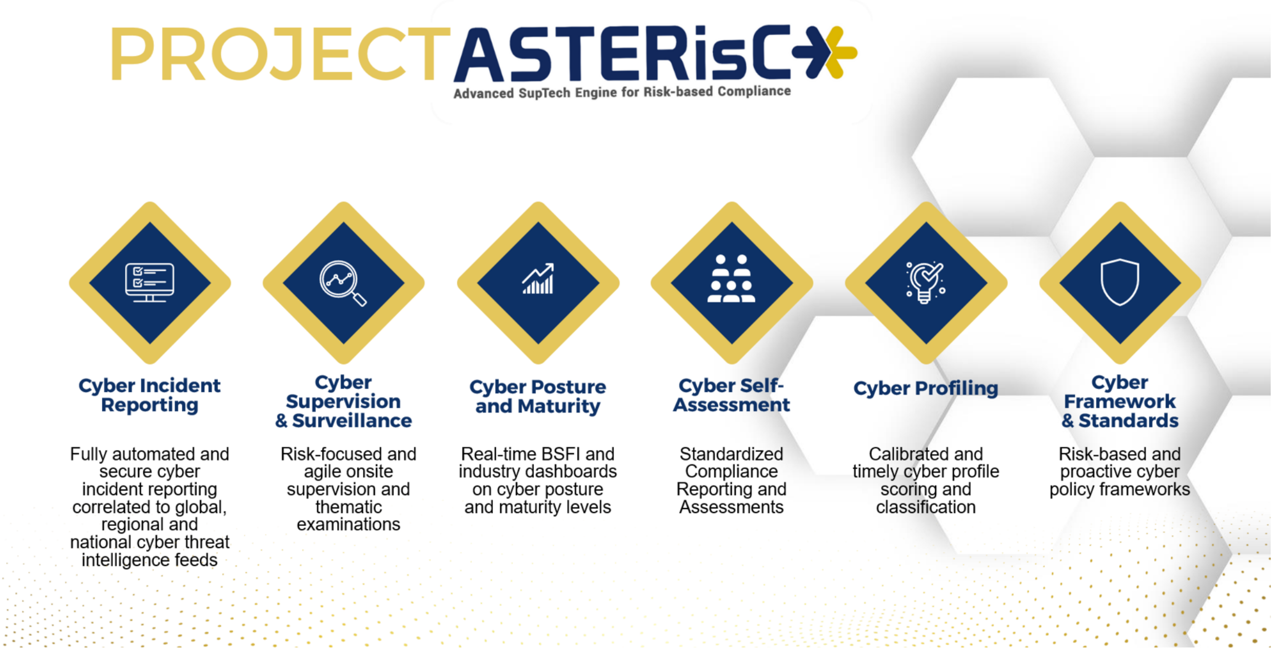
BIS Innovation Network (BISIN) Working Group on Cybersecurity. The BSP is also a member of the BISIN WG on Cybersecurity, which currently consists of sixteen (16) central banks from various regions. BISIN enables central banks' experts to exchange views, discuss technology trends, and to inform on member's latest projects and initiatives on cybersecurity. The BISIN also works on pilots and proof of concepts to explore cybersecurity dimensions of new and emerging technologies.

Figure 3. BSP Collaborative Partnerships

FORTIFYING **SURVEILLANCE CAPABILITIES**

Cognizant of the need to develop capabilities to effectively supervise the evolving digital and cyberthreat landscape, the BSP has taken concrete actions to elevate its technology and cybersecurity risk supervision and surveillance. In 2016, the BSP created a dedicated unit focused on cybersecurity supervision and oversight, later expanded to the Cybersecurity Supervision and Oversight Group (CSOG) in 2018. CSOG handles the end-to-end processes of cybersecurity supervision from policy development, research, onsite supervision including investigation of major cyber-incidents, offsite surveillance, and threat monitoring.

As a testament to BSP's strong commitment in harnessing Regulatory Technology (RegTech) tools to drive cybersecurity goals, the BSP launched the Advanced Suptech Engine for Risk-Based Compliance or ASTERisC* in 2022. It is a pioneering cloud-based RegTech and SupTech solution that automates BSP's cybersecurity supervision while easing regulatory compliance of supervised institutions. *Figure 4* shows cybersecurity supervisory processes supported by ASTERisC. It generates real-time dashboards on cyber profiles, compliance gaps, and threat intelligence enabling BSP to deploy early interventions, such as proactive issuance of cyberthreat advisories and engaging industry stakeholders. The BSP won the Cyber Resilience Initiative Award in the 2023 FinTech & RegTech Global Awards[7] for the implementation of ASTERisC.



Cyber Incident Reporting
Fully automated and secure cyber incident reporting correlated to global, regional and national cyber threat intelligence feeds

Cyber Supervision & Surveillance
Risk-focused and agile onsite supervision and thematic examinations

Cyber Posture and Maturity
Real-time BSFI and industry dashboards on cyber posture and maturity levels

Cyber Self-Assessment
Standardized Compliance Reporting and Assessments

Cyber Profiling
Calibrated and timely cyber profile scoring and classification

Cyber Framework & Standards
Risk-based and proactive cyber policy frameworks

Figure 4. Cybersecurity Supervision Processes Supported by ASTERisC

> *With ASTERisC, the BSP can be more proactive in deploying early interventions and engaging relevant industry stakeholders on cybersecurity.*
>
> *-BSP Deputy Governor Chuchi G. Fonacier*

As part of capacitating BSFIs, the BSP holds regular cyber fora for the Chief Information Security Officers (CISOs) and cybersecurity officers of BSFIs. The cyber fora cover key emerging cybersecurity threats and concerns, which are of utmost importance for the BSFIs to consider in their respective cybersecurity programs. The forum also served as a venue for information sharing and exchange which further bolsters trust and cooperation among the BSFIs.

Lastly, the BSP continues to provide technical/specialized training and education programs to ensure continuous upgrade of the skills, proficiency, and capability of cybersecurity supervisors vis-à-vis cybersecurity developments.

FSCRP Strategy FRAMEWORK

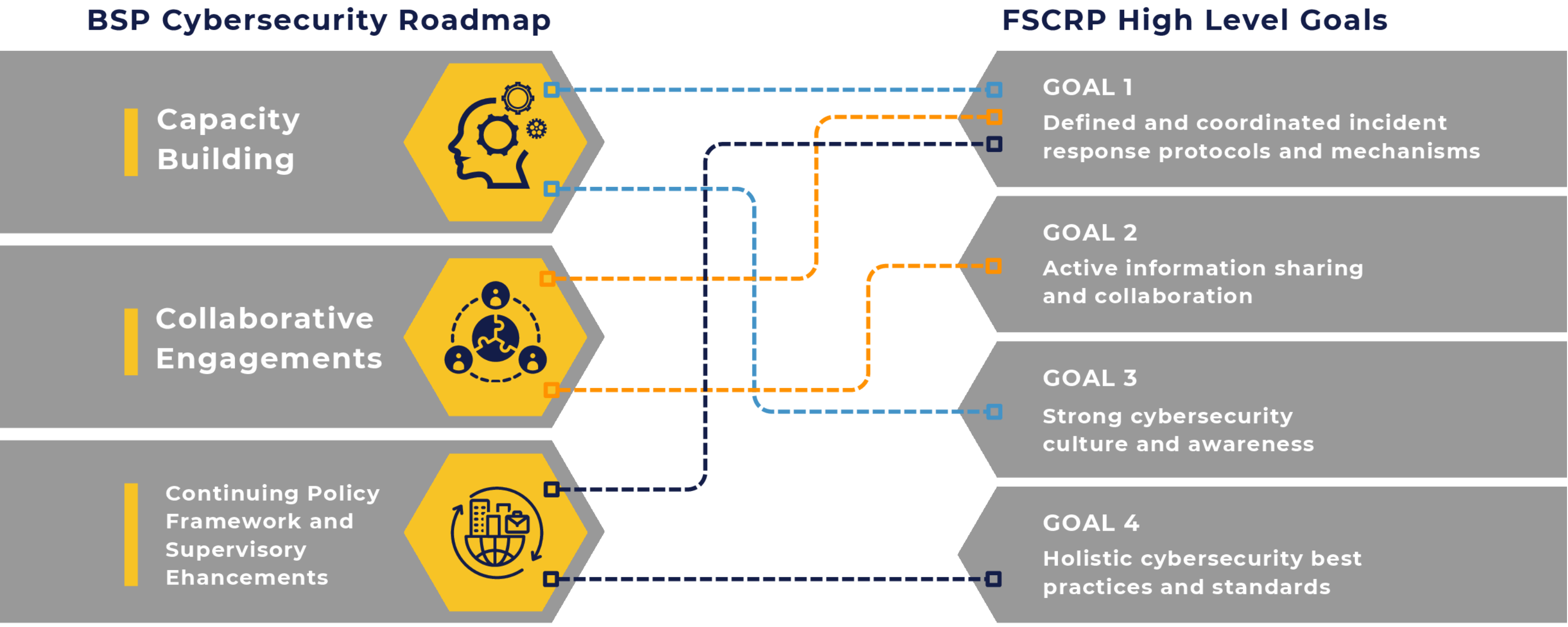

BSP Cybersecurity Roadmap
FSCRP High Level Goals
Capacity Building
Collaborative Engagements
Continuing Policy Framework and Supervisory Ehancements
GOAL 1
Defined and coordinated incident response protocols and mechanisms
GOAL 2
Active information sharing and collaboration
GOAL 3
Strong cybersecurity culture and awareness
GOAL 4
Holistic cybersecurity best practices and standards

Figure 5. FSCRP Strategy Framework Alignment

Taking off from the gains and initial groundwork on cybersecurity, the FSCRP endeavors to further deepen cyber resilience across four main goals or strategic areas. The BSP Cybersecurity Roadmap serves as a jump-off point for the FSCRP. *Figure 5* shows the linkages of the BSP Cybersecurity Roadmap to the FSCRP High Level Goals.

The FSCRP goals and priority actions are shaped by the BSP's engagement with the BSFIs and industry associations as well as stakeholder consultations.

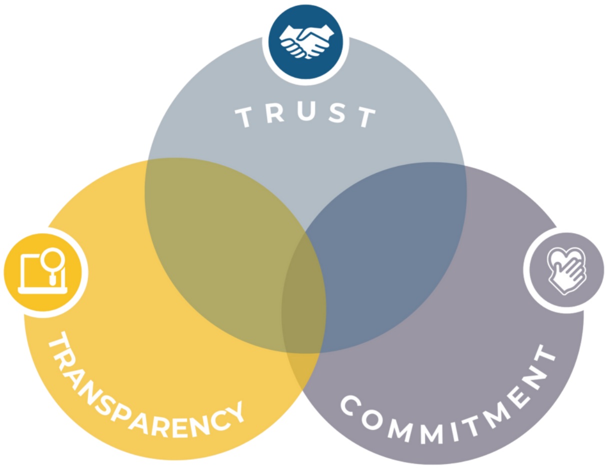


Figure 6. FSCRP Foundational Elements

Core principles on trust, transparency, and commitment serve as foundational elements of the FSCRP to ensure the achievement of its goals (*Figure 6*). It is imperative for industry players to build trust in the financial community in order to further deepen information sharing and collaboration. Engendering trust also means that industry players are aware of and abide by the protocols on confidentiality and data privacy. The core principle on transparency relates to the open communication among industry players and in shaping industry solutions and initiatives under the FSCRP. Transparency also means clear guidance, signal, and direction from the BSP in policy and supervisory development. Commitment among industry players is a key ingredient to ensure that FSCRP goals and initiatives have the necessary resources in terms of finances, manpower, and oversight mechanisms. A strong commitment shall likewise drive the industry to espouse a more mature cybersecurity culture leading to greater alignment with BSP's core goals on financial inclusion, responsible innovation, and financial stability.

FSCRP Governance & Oversight Mechanisms

To ensure strong management commitment and support for the FSCRP, a high-level governance body shall be created to oversee the implementation of the FSCRP and push for the cyber resilience agenda in the financial services industry. Toward this end, a Financial Cyber Resilience Governance Council (FCRGC) shall be established composed of board and executive level officers of relevant industry associations and select systemically important BSFIs and BSP senior management. The FCRGC shall meet at least quarterly to discuss FSCRP implementation and progress, adjust priority initiatives, and provide overall guidance in pushing for necessary industrywide reforms on cybersecurity.

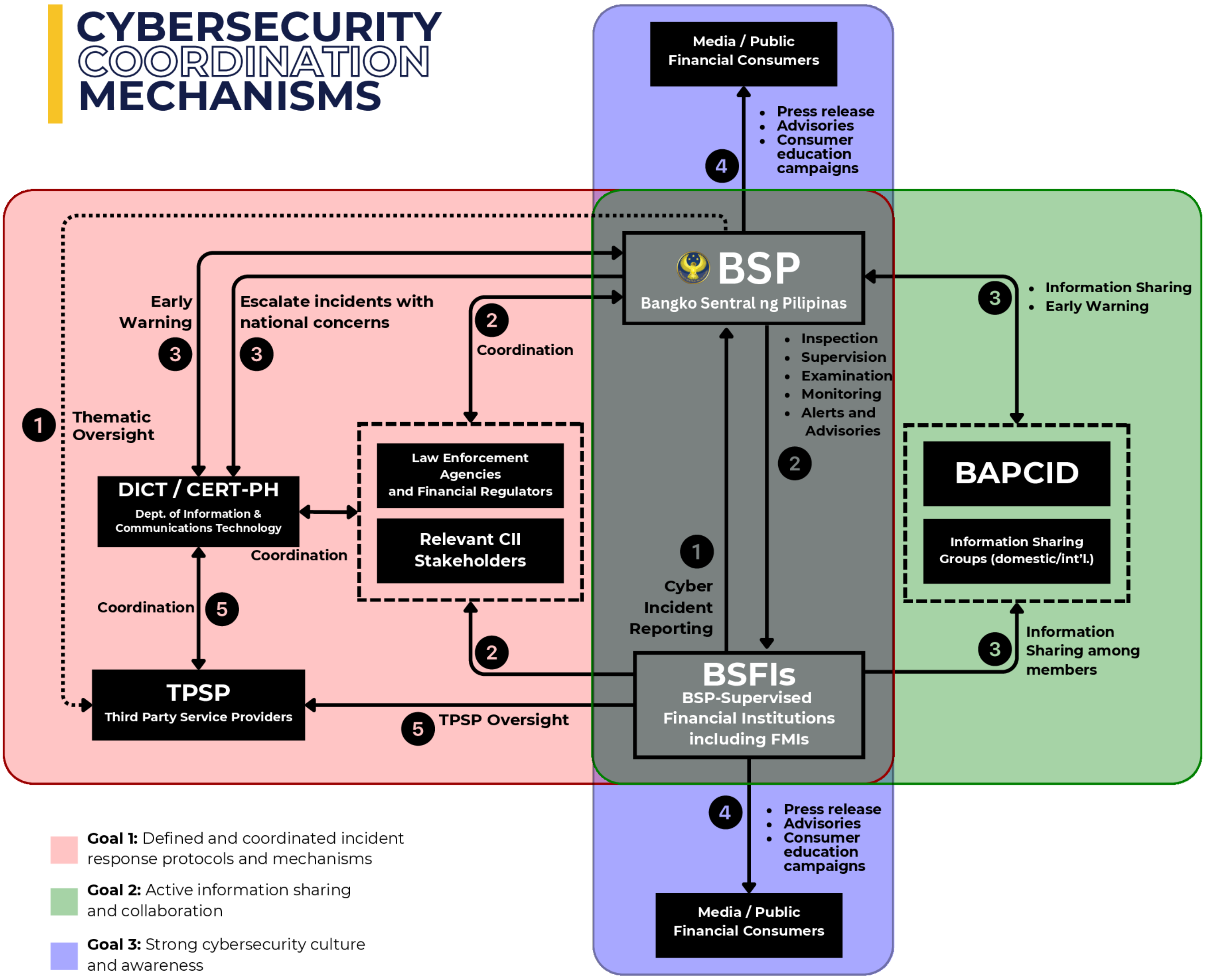
To address broader financial stability concerns on cybersecurity in the financial sector, the BSP shall engage financial regulators on cybersecurity agenda through the Financial Sector Forum[8] (FSF). For national cybersecurity concerns, the BSP shall actively collaborate with relevant government and law enforcement agencies through NCIAC and CERT-PH.

CHARTING THE FSCRP

HIGH-LEVEL GOALS AND ROADMAP

The general work on supervision, incident reporting, and coordination for cybersecurity is a complex process involving various stakeholders to include the BSP, the BSFIs, industry associations, law enforcement agencies and other government offices, third party service providers, various international and domestic information sharing groups, financial clients, and the general public/media. *Figure 7* depicts the typical flow of cybersecurity information and interaction among the stakeholders.

CYBERSECURITY COORDINATION MECHANISMS


Media / Public
Financial Consumers
4
• Press release
• Advisories
• Consumer education campaigns
BSP
Bangko Sentral ng Pilipinas
Early Warning
3
Escalate incidents with national concerns
3
2
Coordination
3
• Information Sharing
• Early Warning
1
Thematic Oversight
• Inspection
• Supervision
• Examination
• Monitoring
• Alerts and Advisories
2
DICT / CERT-PH
Dept. of Information & Communications Technology
Law Enforcement Agencies and Financial Regulators
Relevant CII Stakeholders
Coordination
BAPCID
Information Sharing Groups (domestic/int'l.)
1
Cyber Incident Reporting
Coordination
5
2
TPSP
Third Party Service Providers
5
TPSP Oversight
BSFIs
BSP-Supervised Financial Institutions including FMIs
3
Information Sharing among members
4
• Press release
• Advisories
• Consumer education campaigns
Media / Public
Financial Consumers

🟥 **Goal 1:** Defined and coordinated incident response protocols and mechanisms

🟩 **Goal 2:** Active information sharing and collaboration

🟦 **Goal 3:** Strong cybersecurity culture and awareness

⬛ **Goal 4:** Holistic cybersecurity best practices and standards

Figure 7. Cybersecurity Coordination Mechanisms

1 As a starting point, the BSP collects cyber threat information from the BSFIs through regulatory cyber incident reporting requirements as prescribed under BSP Circular 1019. The BSP also receives cyber threat intelligence from various sources, such as through information sharing groups/associations here and abroad, cybersecurity providers, and the DICT/CERT-PH. The information gathered by BSP are then analyzed further which feed into BSP's cybersecurity supervision and oversight processes.

2 Depending on the severity of the cyber incident, an overseeing examination or offsite monitoring and coordination may be warranted to proactively address concerns. Coordination with law enforcement agencies, such as the National Bureau of Investigation (NBI), Philippine National Police (PNP), Department of Justice (DOJ), and other financial regulators may be necessary to capture and prosecute cyberthreat actors and to recover cyber fraud losses.

3 On a broader scale, the BSP shares specific cyberthreat advisories to serve as early warning to prevent further exposure from active cyber threats and frauds. These are being shared primarily through the BAPCID and domestic and international information sharing groups, including the CERT-PH for those with national security implications. The BSP also coordinates with various domestic and international groups for benchmarking and knowledge exchange. On the other hand, certain BSFIs share anonymized cyberthreat intelligence, best practices, and experiences through BAPCID.

4 As part of the BSP's consumer awareness and education efforts, the BSP issues public advisories and press releases to keep the banking public aware and to prevent them from falling victims to existing and emerging cyber fraud and threats. This is to complement BSFIs' cybersecurity awareness and education programs for their clients.

5 Lastly, BSFIs have the responsibility to exercise oversight on its vendors or third-party service providers to promote cyber resilience. The BSFIs' outsourcing and TPSP risk management is also one of the IT risk areas assessed by the BSP as part of onsite/offsite supervision. The BSP also conducts thematic reviews on major service providers, specifically those providing critical services to multiple BSFIs to address potential systemic risks. On the other hand, certain service providers may need to coordinate with the DICT or their respective regulator, particularly if they are considered as CII (e.g., telecommunications companies, power companies).

The FSCRP goals cut across the whole cybersecurity network and domains. As shown in *Figure 7*, there are certain overlaps in each of the goals indicating that the goals reinforce and supplement each other. For example, conducting industrywide cybersecurity testing exercises largely enhances incident response mechanisms under Goal 1, but this could also contribute to enhancing cybersecurity culture and capacity of the industry players pursued under Goal 3.

Likewise, information sharing and collaboration efforts under Goal 2 feed into the industry incident response protocols and mechanisms under Goal 1 as well as provide key inputs for BSP's policy development processes under Goal 4. These interdependencies only highlight that the FSCRP goals should be considered holistically and that it is crucial to pursue each of the goals with the same degree of commitment and dedication.

While BSP regulations provide adequate guidance on incident response capabilities and requirements for individual BSFIs to effectively manage major cyber attacks, there is a need to come up with industrywide incident response protocols to address interdependencies and systemic risks. This becomes even more important as connectivity, customer digital touchpoints, and emerging technologies proliferate across the financial services network. Effective cyber incident response and recovery demands a coordinated effort among multiple industry players. A pivotal approach to realizing this objective is to develop comprehensive plans and conduct extensive tests to ensure continuing improvement.

GOAL ONE

DEFINED AND COORDINATED INCIDENT RESPONSE PROTOCOLS AND MECHANISMS

Priority Action D1. Establish baseline industry Incident Response Plan
Target timeline. 2024 - 2026

Key Milestones	Year
Inventory/mapping of critical FIs/interdependencies	2024
Identification of cyber risk concentrations	
Baseline incident response plan research and development incorporating criticality of BSFIs and interdependencies	2025
Exposure of the draft plan	
Finalization and cascading of the plan to BSFIs	2026
Rollout of training and awareness program	

To serve as a baseline for industry response and coordination, an industrywide cyber incident response plan shall be established. Said plan shall cover, at a minimum, triggers for activation, escalation protocols among relevant stakeholders, and crisis communications. Key inputs to this plan include identifying mission-critical systems, services, and interdependencies in the industry. Mapping and analyses of concentration of cyber risk exposures shall also be performed that will inform the incident response plan procedures and mechanisms. The plan shall be based on global best practices and standards on incident response and shall cover the entire incident response lifecycle in *Figure 8*.

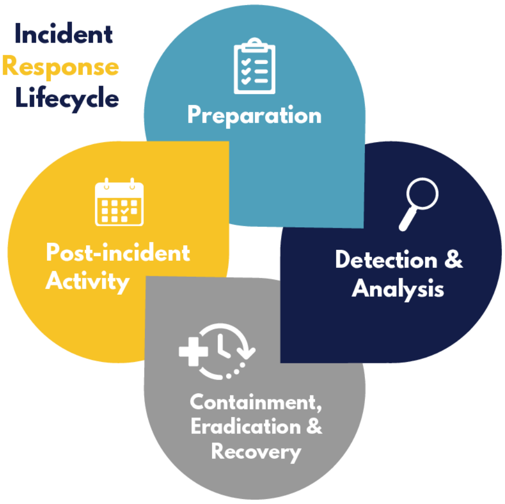


Figure 8. Incident Response Lifecycle

Priority Action D2. Develop scenario-based incident response playbooks
Target timeline. 2024 - 2029

Key Milestones	Year
Development of playbook on Data Breach	2024
Development of playbook on Supply-Chain Attacks	2025
Development of playbook on Application Programming Interface Exploit	2026
(To be determined, depending on emerging threats)	2027 to 2029

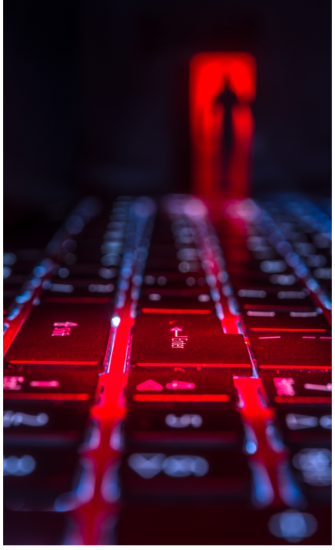
The industry incident response plan shall be supplemented by scenario-based incident response playbooks. A cybersecurity playbook is a document that provides detailed information on a specific cybersecurity incident type that prepares and familiarizes incident responders on the adequate action to minimize or eliminate further damage. In 2021, the BSP, in coordination with BAP, issued an Industry Cybersecurity Playbook Development Guide on ransomware attacks. The playbook serves as a practical guide to the industry in developing and enhancing their own cyber incident response playbooks in effectively responding to ransomware attacks. For 2024 to 2029, scenario-based industry playbooks shall be developed covering emerging cyberthreats (e.g., data breaches, advanced persistent threat (APT) attacks) requiring specific and actionable guidelines and recommendations.

Playbook Recommended Contents

- **General description and mechanics of the cyber incident scenario;**
- **Incident handling process;**
- **Roles and responsibilities:**
  - **Authority to declare a cybersecurity incident and initiate the playbook; and**
  - **Subject matter experts (SME) and/or personnel responsible for each phase on the incident handling process;**
- **Triggers for the detection and for the alternative courses of action;**
- **Response timeline or turnaround time;**
- **Allocated budget for remediation and the required approval for emergency response situations; and**
- **Directory and contact information of organizations, government agencies or individuals.**

Priority Action D3. Conduct progressive industrywide cyber testing exercise regime
Target timeline. 2024- 2029

Key Milestones	Year
Progressive industrywide cyber testing exercise program and pilot cyber testing exercise	2024
Industry tabletop exercise	2025
Simulated scenario testing exercise	2026
Annual testing exercises, including red-team test and scenario-based test	2027 to 2029



The evolving nature and sophistication of cyber threats and attacks compels industry players to continually improve cyber defenses and capabilities. One of the ways where cyber maturity can be methodically assessed and measured is through cyber testing exercises, either individually by the BSFIs or as an industry, to test interdependencies/coordination especially for system-wide cyber-attacks.

The BSP is currently studying the existing regulatory frameworks on cyber-testing and is exploring ways to tighten supervisory expectations/requirements. These include more stringent and clear requirements for vulnerability assessment and penetration testing (VAPT), red team testing, and compromise assessments, among others. The BSP is also studying the European Central Bank (ECB) model for the Threat Intelligence-based Ethical Red Teaming of the European Central Bank (TIBER-EU) red team testing framework and the Bank of England Critical National Infrastructure Banking Supervision and Evaluation Testing (CBEST) threat intelligence led assessments for possible implementation in the Philippines.

To further deepen industry cyber resilience and readiness, a program shall be developed for the regular conduct of industrywide and progressive cybersecurity testing exercises as informed by surveillance activities. These include tabletop simulated testing, scenario based testing and red team testing covering both technical and governance/process-based tracks.

Priority Action D4. Explore setting up of an industry Security Operations Center (SOC)
Target timeline. 2024-2026

Key Milestones	Year
Conduct of benchmarking study and research on industry SOC implementation of other jurisdictions	2024
Consultation with industry associations and BSFIs	2025
Identification of resource requirements and conduct of feasibility study	
Finalization of recommendation	2026

To enhance situational awareness, threat visibility, as well as activate a more proactive response to identified threats, the feasibility of setting up an industry SOC shall be explored.

To assess the feasibility of the setup, a phased approach will be adopted where the capability of the industry SOC would initially collect relevant log information/details from the respective Security Incident and Event Management (SIEM) of pilot participants, such as systemically important BSFIs. These data points are then analyzed for anomalies and potential indicators of compromise (IOCs) for sharing with the concerned BSFI and the industry participants for proactive remediation/response. Once the pilot is successful and meets target objectives, then a full-blown industry SOC would be pursued covering a wider set of participating BSFIs. Another model that may be explored is a full-service industry SOC catering to smaller financial institutions, to further enhance their capabilities against evolving threat actors. This setup is also aligned with the National Cybersecurity Plan 2023-2028 by the DICT in Figure 9 where a proposed connection from Sectoral CERT flows through the National CERT and the National Cyber Intelligence Network (Cyber fusion SOC).

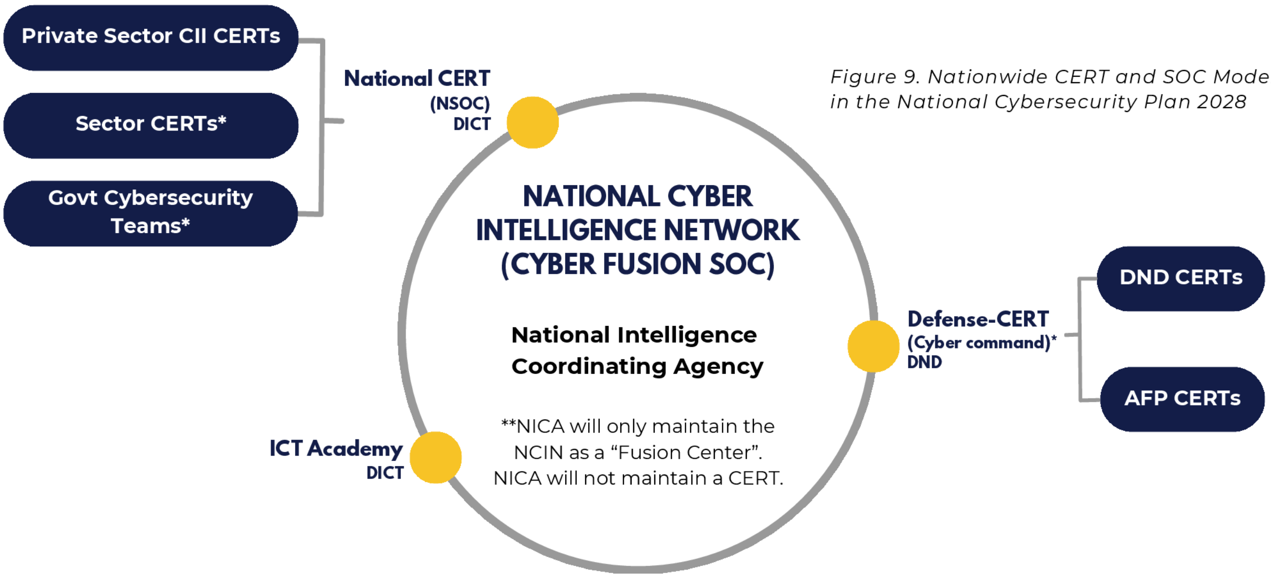

Private Sector CII CERTs
Sector CERTs*
Govt Cybersecurity Teams*
National CERT
(NSOC)
DICT
NATIONAL CYBER INTELLIGENCE NETWORK (CYBER FUSION SOC)
National Intelligence Coordinating Agency
**NICA will only maintain the NCIN as a "Fusion Center". NICA will not maintain a CERT.
ICT Academy
DICT
Defense-CERT
(Cyber command)*
DND
DND CERTs
AFP CERTs

Figure 9. Nationwide CERT and SOC Model in the National Cybersecurity Plan 2028

BSP AS LEAD CERT FOR THE BANKING SECTOR

The Department of Information Communications Technology (DICT), under Department Circular No. 003 series of 2020, designated the Bangko Sentral ng Pilipinas as the Lead Computer Emergency Response Team (CERT) for the Banking Sector. This is in line with Section 29 of the Implementing Rules and Regulations of the Republic Act (R.A.) No. 10175, otherwise known as the "Cybercrime Prevention Act of 2012", mandating the creation of the CERT. Furthermore, the National Cybersecurity Plan 2022 laid down the establishment of the National CERT and the respective Sectoral CERTs.

The functions of the BSP as Sectoral Lead CERT include four key areas:

- Promulgate policies, guidelines, and programs to advance cyber resilience;
- Promote information sharing and collaboration;
- Perform supervisory functions on major cyber incidents; and
- Escalate incidents bordering on national security to CERT-PH.

Considering the sensitive nature of financial transactions, including compliance with laws on bank secrecy of deposits, the reporting of cyber incidents and other cyberthreat-related statistics to the CERT-PH/DICT shall be subject to existing rules on data privacy and confidentiality of information.

The Cybersecurity Supervision and Oversight Group of the Technology Risk and Innovation Supervision Department (TRISD) is primarily responsible for the BSP's Sectoral CERT roles and functions.

GOAL TWO

ACTIVE INFORMATION SHARING AND COLLABORATION

With the dynamic and evolving cyberthreat environment, it is imperative for the BSP, BSFIs, and industry stakeholders to engage in open, intelligence-led, and actionable information - sharing platforms and mechanisms. Through interactive exchange of cyberthreat intelligence, cybersecurity best practices and developments, the industry is moving closer to achieving enhanced situational awareness, and improved threat detection and response. This undertaking also accentuates the importance of maintaining the integrity and timeliness of information, sharing of information without fear of judgment or retribution, and sustaining the exchange of information.

Priority Action A1. Expand and further enhance BAPCID as an industry-sharing platform
Target timeline. 2024 - 2029

Key Milestones	Year
Coordination with BAP and industry associations on the expansion strategy and address relevant concerns	2024
Study of potential linkages to other information sharing platforms in other identified industries/jurisdictions.	2025
Enhancement of cybersecurity dashboards in ASTERisC for sharing in BAPCID platform	2026
Overseeing of engagement of BSFIs in BAPCID	2024 to 2029

Since the issuance of BSP Circular 982 mandating information sharing and collaboration among BSFIs, collaborative engagements were established to actively share cyberthreat information and best practices. A major milestone in this endeavor is the establishment of the Bankers Association of the Philippines Cybersecurity Incident Database (BAPCID) in 2018. BAPCID is an industry cyber threat and best practices sharing platform hosted by the BAP. It is a web-based and highly secure portal through which participants can anonymously report incidents and threats. Through BAPCID, BSFIs can raise the level of situational awareness on actionable information related to latest tactics, techniques, and procedures (TTPs) of cyberthreat actors targeting financial institutions, critical vulnerabilities, and other relevant data, including those hosted in the darkweb. The BSP, as an advisory member, uses BAPCID as a platform to share issuances on specific cyberthreats as well as approved memoranda for restricted distribution.

Seeing the benefits of such a platform, even for small to medium-sized financial institutions, the BSP expanded coverage of BSFIs and encouraged participation to the BAPCID through Memorandum No. M-2019-016 dated 11 June 2019. Further, in line with the mandate of the DICT under Department Circular 003, the BSP required participation of identified BSFIs taking into account their IT profile complexity, systemic importance, and cyberthreat profiles. Said expansion enhanced cyberthreat visibility as well as facilitated coordination efforts in proactively responding to major cyber incidents and threats. At present, there sixty (60) financial institutions connected to BAPCID, including the BSP, Chamber of Thrift Banks (CTB), and Rural Bankers Association of the Philippines (RBAP) as advisory/industry members.

To further enhance the extent and the depth of intelligence sharing in the financial community, the BSP seeks to position BAPCID as a central intelligence sharing platform for the financial services industry. Information sharing platforms may emanate from other sectors in the industry (e.g., fintech companies, digital banks, CTB, RBAP) but eventually, these shall be linked to BAPCID.

To complement BAPCID, the BSP shall leverage on ASTERisC's capabilities to provide industry cyber dashboards and maturity index reports, which shall be shared with BAPCID users. The BSP shall also link cyber threat intelligence and surveillance feeds from BSP's cyber threat surveillance and from the proposed industry SOC, if this will materialize.

On a broader scale, the Philippines may study the merits of the passage of laws on information sharing, which aim to promote and foster nationwide cyber situational awareness, preparedness, and threat intelligence among various private and government stakeholders.

Priority Action A2. Strengthen and forge strategic partnerships in domestic and international fora
Target timeline. 2024 – 2029

Key Milestones	Year
Engage industry associations on proposed initiative on fraud information sharing (dependent on passing of AFASA bill)	2024 to 2025
Strengthen coordination with telco industry	2026 to 2027
Develop MOU for cyber coordination with CERT-PH and other relevant agencies	2024 to 2025
Continue active participation and engagement with domestic and international fora	2024 to 2029

To build on the existing level of trust and cooperation, the BSP shall continue to strengthen and forge strategic partnerships aimed at pushing industrywide reforms and addressing pain points in all aspects of cybersecurity.

In BSP's active engagement with counterparts in both domestic and international forums, key industrywide initiatives are being proposed by various industry associations. Highlights of the proposals are in *Figure 10*. The BSP aims to take these initial discussions to the next level and come up with concrete, viable, and time-bound solutions for implementation by relevant stakeholders.

Proposed Industry Initiative	High Level Summary/Overview
Central Fraud Information Sharing Platform (inc. Money Mule Database)	This initiative aims to establish a central database of verified mule accounts, as confirmed by individual BSFI's investigation. The industry shall use the shared database in conducting Know-Your-Customer (KYC) procedures for new depositors/clients and in performing Enhanced Due Diligence (EDD) as part of the regular AML monitoring for existing clients. This mechanism will prevent verified mule accountholders to open accounts and perform financial transactions with BSFIs which would significantly enhance integrity in the financial system. However, due care must be undertaken, and a judicious process must be established in the design of the central database to ensure that the blacklist would not unduly deny financial services to legitimate financial consumers (e.g. victims of phishing whose accounts received fraudulent funds). On top of the money mule database, sharing of fraud information, such as technical details on IP address, device ID (International Mobile Equipment Identity (IMEI), brand and model) may be pursued. These data can be linked to the fraud management systems of BSFIs as inputs for fraud risk calculations and corresponding anti-fraud actions. Other areas for fraud information sharing include fraud investigation, temporary holding of funds, and recovery of losses by financial consumers.
Coordination with Telecommunications Industry to Address Smishing and SMS spoofing attacks, as well as coordination for cyber investigation	Phishing attacks, also known as Smishing, are increasingly being carried out via the Short Message Service (SMS) system. In addition, SMS spoofing, a scheme where the sender ID is made to appear a legitimate sender, is executed in combination with Smishing to defraud financial clients. In such cases, financial consumers can be easily victimized since the fraudulent messages are co-mingled with the previous genuine/legitimate messages from the BSFI. While the Philippines already enacted the SIM Card Registration Law under R.A. 11934, there are still some areas that need further enhancement to ensure that mobile phone users are properly onboarded and verified. In this manner, phishing offenders and scammers can be easily traced and apprehended. The BSP, together with the financial services industry, seeks to collaborate with the telecommunications companies (telcos), through the National Telecommunications Commission (NTC), in exploring holistic solutions to address these concerns.

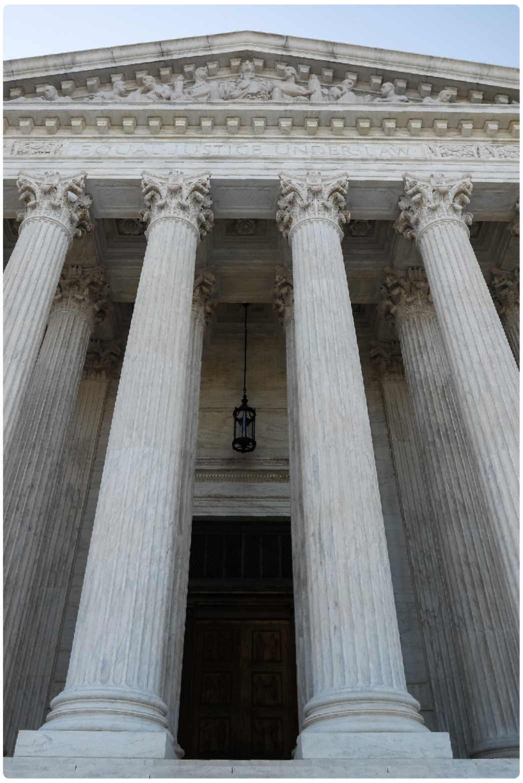
Figure 10. Planned Industry Initiatives on Cybersecurity

Priority Action A3. Support the passing of cyber-related legislative initiatives
Target timeline. 2024 – 2027

Key Milestones	Year
Passage of the AFASA Bill and crafting of its IRR	2024 to 2025
Passage of the Amended Bank Secrecy Laws and crafting of its IRR	2026 to 2027

To further strengthen financial consumer protection and integrity within the financial system, the BSP actively works with the BSFIs and lawmakers for the passing of cyber-related legislative initiatives. In particular, the BSP is pushing for the passage of the "Anti-Financial Account Scamming Act" (AFASA). The bill aims to deter financial cybercriminals by regulating and criminalizing the acts of money mules and social engineering schemes. The proposed Bill also includes provisions that would enhance the conduct of fraud investigations and coordination with law enforcement agencies to catch and apprehend cyber criminals to the fullest extent of the law.

The BSP is also closely working with lawmakers to liberalize the Bank Secrecy Law, which is currently being abused by cyber threat actors and scammers. As an illustration, a court order is required for the victims to pursue legal claims against cyber offenders. However, this may be a challenge as BSFIs cannot disclose the name of the depositor and other deposit information subject to bank secrecy laws. Given these hurdles, it is quite difficult to go after and prosecute threat actors. Thus, amending this law is necessary to ensure equal protection for financial consumers victimized by fraud and scams.



Priority Action S1. Develop and implement cyber education program for BSFI Board and Senior Management
Target timeline. 2024 – 2029

Key Milestones	Year
Consultation with industry associations and BSFIs	2024
Current state assessment / survey on individual BSFI cyber education program for Board and Senior Management	2025
Recommend/develop cyber education program for Board and Senior Management and establish success metrics	2026
Implement and monitor	2027 to 2029

In line with the board and senior management's crucial role in fostering a strong cybersecurity culture in their respective institutions, a cyber education program designed for senior level executives will be designed and implemented. The program is a continuing initiative covering formal learning sessions, regular roundtable discussions and one-on-one in-depth sessions with the BSP to further sensitize the Board and senior management on cybersecurity matters and concerns. Topics for discussion include updates on the cyberthreat landscape, cybersecurity roles and responsibilities, governance requirements, incident response and cyber training and awareness. The program can also be tied with the industry cyber testing under Goal 1, particularly on testing cyber incident response under the governance track. The BSP shall tap and coordinate with relevant groups and associations, such as the Bankers Institute of the Philippines (BAIPHIL), BAP and ISOG in developing and implementing the program.

GOAL THREE

STRONG CYBERSECURITY CULTURE AND AWARENESS

This goal covers strengthening the people element in the information security chain. As a core foundation for strong cyber resilience, a mature cybersecurity culture and heightened awareness is necessary among BSFIs' top management, CISOs, employees and officers and financial consumers. A holistic approach should likewise be adopted in ensuring adequate supply of cybersecurity skills and talents are available to meet the industry's existing and future cybersecurity needs. In a report on "National Cybersecurity Talent Workforce Assessment Report of the Philippines"[9], concerns raised include the lack of cybersecurity professionals, lack of curriculum feedback loops between the industry and academia, no incentive for academia to ramp-up its cyber pipeline, and no incentive for the industry for cyber skills development, among others.

Priority Action S2. Regularly conduct CISO/cyber forum and Annual Cybersecurity Summit
Target timeline. 2024 – 2029 (Continuing Engagement)

In 2021, the BSP initiated the conduct of CISO/cyber forum in line with BSP's pursuit to foster trust and collaboration among BSFIs to achieve industry cyber resilience. Since the initial run of the forum, it has served as an avenue for the BSP to discuss emerging cyberthreat concerns and developments and actively engage the CISOs and cybersecurity officers, who are the BSP's immediate contact points for urgent cyber-related matters.

The BSP shall continue to regularly provide such cyber fora to drive industry initiatives under the FSCRP, update the CISOs and cybersecurity officer on recent regulations and guidelines, and provide a platform for round-table discussion on cybersecurity issues in the industry. To further deepen collaboration, a CISO or Cyber Network may be created where CISOs can engage with each other on cyber-related matters.

Priority Action S3. Conduct cybersecurity roadshows for small and medium-sized FIs
Target timeline. 2024 – 2027

Key Milestones	Year
Develop/update materials for cybersecurity roadshows	2024
Conduct roadshow sessions in various regions to meet 100% of target BSFI participants	2024 to 2027

To enhance the cyber capabilities of relevant officers from small to medium-sized BSFIs, the BSP, in coordination with the relevant bankers' federations and groups, shall conduct roadshows covering topics on IT fundamentals and baseline regulatory expectations on cybersecurity, digital innovation, fraud risk management, cloud computing, and IT outsourcing risk management, among others.

The roadshow also aims to highlight sound IT and cybersecurity risk management practices, which smaller BSFIs can adopt in their digital transformation initiatives. This will also serve as an avenue for BSFIs, especially those with simple and moderate IT profile complexity that are not regularly examined by TRISD, to discuss their concerns and clarifications on IT and cybersecurity regulations and good practices.

ROADSHOW

BSP CYBERSECURITY & IT RISK FUNDAMENTALS
ROADSHOW 2024

17-18 APRIL 2024
DAVAO CITY

29-30 MAY 2024
CAGAYAN DE ORO

Priority Action S4. Pursue holistic programs for cybersecurity skills and talent development
Target timeline. 2024 – 2029

Key Milestones	Year
Research best practices on cybersecurity skills development	2024
Establish competency framework to guide the financial sector in building cyber-capabilities	2025 to 2026
Engage the academe and industry for collaborative cyber capacity building and education programs	2027 to 2029

To ensure the continuous supply of high caliber cybersecurity professionals and talents in the industry in the cybersecurity workforce, the BSP shall develop a holistic cybersecurity skills development program aimed at enhancing cybersecurity skills for technical, risk, and management tracks. In pursuing said programs, the BSP shall ensure diversity in the workforce, which provides equal opportunities for workers of different age groups, gender, culture and social backgrounds. The BSP shall likewise offer apprenticeship program focused on cybersecurity for fresh graduates and/or young professionals wishing to venture into cybersecurity.

The financial services industry may pursue partnerships with academic institutions/training providers to develop specialized hands-on programs on cybersecurity. To support the national cyber skills agenda, the BSP may collaborate with the Department of Information and Communications Technology (DICT), Commission on Higher Education (CHED), BAIPHIL, and select schools and universities to design cybersecurity-related courses that meet the specific needs of the financial services industry. A standard competency framework for cybersecurity may be adopted by the financial sector aligned with international best practices and frameworks such as the US National Initiative for Cybersecurity Education (NICE) framework[10] *(Figure 11).*

Workforce Framework for Cybersecurity (NICE Framework)

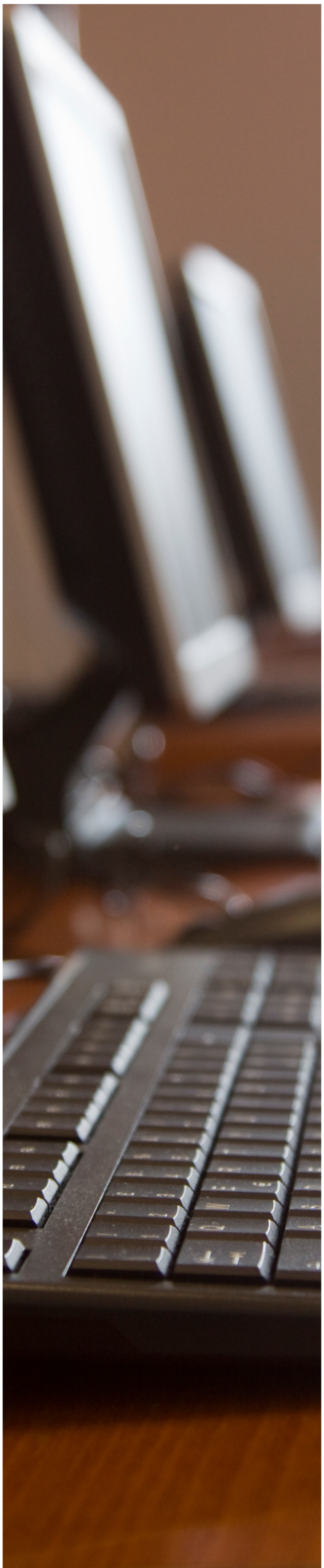
The Workforce Framework for Cybersecurity, commonly referred to as the NICE Framework, is a nationally focused resource to help employers develop their cybersecurity workforce. It establishes a common lexicon that describes cybersecurity work and workers regardless of where or for whom the work is performed. The NICE Framework applies across public, private, and academic sectors.

The NICE Framework is comprised of the following components:
- Categories (7) – A high-level grouping of common cybersecurity functions
- Specialty Areas (33) – Distinct areas of cybersecurity work
- Work Roles (52) – The most detailed groupings of cybersecurity work comprised of specific knowledge, skills, and abilities (KSAs) required to perform tasks in a Work Role

Figure 11. NICE Framework

Priority Action S5. Mainstream cyber education and awareness programs for financial clients.
Target timeline. 2024 - 2029

Key Milestones	Year
Proposal for the creation of a dedicated website for cybersecurity awareness for the public.	2024
Site design and development	2025
Content development and management	2026 to 2029



To ensure that financial consumers are equipped with the right tools and know-how to properly optimize the use of digital financial channels and avoid being victims of cyber fraud and scams, the BSP, with the technical assistance provided by USAID, embarked on a cyber awareness and digital literacy campaign in 2020. With the theme, *#E-Safety is Everyone's Responsibility,* the campaign aims to stress that everyone – from financial regulators, financial services providers, business and individuals – play a key role in keeping digital financial ecosystem safe and secure.

Expanding on this campaign, the BSP shall mainstream cyber education and awareness through various programs and modalities to ensure wider coverage. To enhance its effectiveness, the BSP shall develop customized materials and cyber advisories targeting specific segments of the society, particularly those considered as high-risk and vulnerable to cyber threats and scams (e.g., senior citizens, youth, underprivileged sectors and women). The BSP shall also create a dedicated website that will house a collection of cybersecurity tips, awareness, and education materials, that will be made available to the public. The proposed website shall include cyber hygiene tips and awareness, cyber-related BSP regulations, guidelines and issuances, cyber standards and good practices forum and latest technology and cyber news tab. The website may feature a chatbot with generative pre-training transformers (GPT) capabilities to address questions from the financial clients and the public, in general.

GOAL FOUR

HOLISTIC CYBERSECURITY BEST PRACTICES AND STANDARDS

The financial services industry has been laying the groundwork to achieve a stable and resilient financial system. A key initiative to concretize this vision is the adoption of cybersecurity best practices and standards that encapsulate all cybersecurity domains.

Under this goal, standards and practices are seen to (i) adequately capture and address the evolving cyber-threats; (ii) align with the leading standards and frameworks issued by the standard-setting bodies on information security (e.g., National Institute of Standards and Technology [NIST], International Organization for Standardization [ISO], Control Objectives for Information and Related Technology [COBIT]), when applicable; (iii) follow the practices of other regulatory authorities in economies with advanced cybersecurity capabilities; and (iv) cover people, process, and technology.

Priority Action H1. Complete policy reforms on digital security controls, API security, Cybersecurity Maturity Model Framework, and Supply Chain Risk Management
Target timeline. 2024 – 2026

The BSP shall endeavor to issue policy reforms to better guide BSFIs on managing cyber risks on various domains. Policy initiatives in the pipeline include:

a. Update of digital security controls - This initiative aims to update security control requirements for electronic payment and financial services (EPFS). Said reforms will take into consideration emerging threats and vulnerabilities as well as developments in the digital innovation space.

b. API Security Controls - This policy framework formalizes security control requirements for API implementations to address common and emerging API exploits and vulnerabilities. This policy also prepares the industry to embark on the Open Finance initiative, which is anchored on open API technologies.

c. Cybersecurity Maturity Model Framework (CMM) - To better guide BSFIs to chart their cybersecurity roadmap and targets, the BSP shall draft a cybersecurity maturity model (CMM) framework. Such framework defines four levels of capabilities on critical cybersecurity areas covering key elements from people, policies, processes, and technology.

d. Supply Chain Risk Management - In response to the escalating risks arising from the growing dependence of BSFIs on tools, solutions, and services offered by third-party entities, a policy will be formulated to specifically address the intricacies of the supply chain components. This policy is designed to complement the prevailing outsourcing guidelines, providing a detailed framework to elucidate the security requisites and expectations during the onboarding process of third-party service providers. Additionally, it aims to delineate the ongoing risk management practices essential for ensuring the security and reliability of the IT services and solutions furnished by these external entities.

A study shall likewise be conducted in the areas of technology and security service provider accreditation, vulnerability risk management, and the authority, functions and responsibilities of the Chief Information Security Officer (CISO) and Cybersecurity Office (CYSO), among others, to identify future policy enhancements.

Priority Action H2. Explore establishment of an Industry Cyber Innovation/Research Hub
Target timeline. 2025 – 2027

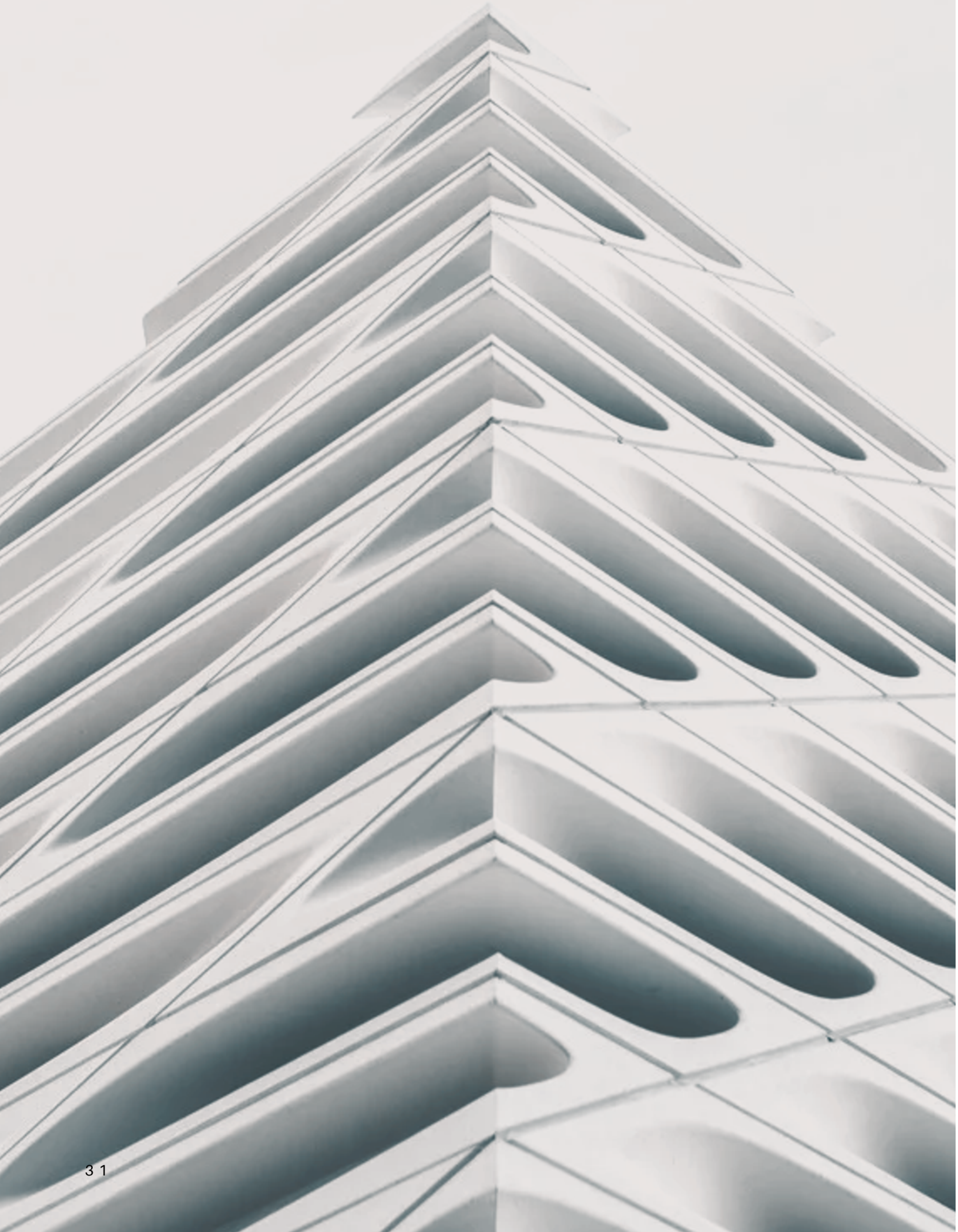
Key Milestones	Year
Research and study implementations of other countries	2025
Conduct feasibility and propose recommendations	2026
Finalize and implement recommendations	2027

To promote a research-oriented culture on cybersecurity, the BSP shall explore the establishment of an industry cyber innovation and research hub. The hub shall feature a digital forensics and technology laboratory where simulation of new vulnerabilities exploitation, cyber attack methodologies, and malware analyses can be performed for policy research, supervisory, and training purposes. Researchers and industry participants can likewise test and analyze emerging technologies to check potential cybersecurity implications and conduct pilots or sandbox applications. The hub shall also include a digital library or website where researchers from the BSP, the BSFIs, and the academe can research on various papers, articles, and curated cybersecurity knowledge base. The BSP, in coordination with industry players, shall likewise endeavor to regularly develop research or white papers focused on various cybersecurity topics and domains.

Priority Action H3. Conduct Benchmarking Exercises on Cyber Capabilities
Target timeline. 2024 – 2025

To ensure that the BSP and the financial services industry are collectively at par with cybersecurity best practices and standards adopted by advanced economies, the BSP shall conduct regular benchmarking exercises, through study visits and capacity building activities, with counterparts in other jurisdictions. For example, the BSP may study the cyber-testing/red team testing regime currently implemented by the European Central Bank. In conjunction with the proposed set of industry-SOC and cyber innovation hub, the BSP may refer to financial supervisors in other countries that are already far ahead in implementation in their respective jurisdictions.

ANNEX



List of Acronyms and Abbreviations

AFASA	Anti-Financial Account Scamming Act
AI	Artificial Intelligence
AML	Anti-Money Laundering
API	Application Programming Interface
APT	Advanced Persistent Threat
ASTERisC	Advanced SupTech Engine for Risk-based Compliance
BAPCID	Bankers Association of the Philippines Cybersecurity Incident Database
BIS	Bank for International Settlements
BSFI	BSP-Supervised Financial Institution
CBEST	Critical National Infrastructure Banking Supervision and Evaluation Testing
CERT	Computer Emergency Response Team
CERT-PH	Philippine National Computer Emergency Response Team
CHED	Commission on Higher Education
CII	Critical Information Infrastructure
CISO	Chief Information Security Officer
CMM	Cybersecurity Maturity Model
COBIT	Control Objectives for Information and Related Technology
CTB	Chamber of Thrift Banks
DDoS	Distributed Denial of Service
DICT	Department of Information & Communications Technology
DOJ	Department of Justice
DTN	Digital Technology Network
EDD	Enhanced Due Diligence
EPFS	Electronic Payments and Financial Services
FCRGC	Financial Cyber Resilience Governance Council
FMI	Financial Market Infrastructure
FSB	Financial Stability Board
FSCRP	Financial Services Cyber Resilience Plan
GPT	Generative Pre-training Transformers
IMEI	International Mobile Equipment Identity
IMF	International Monetary Fund
IOC	Indicators of Compromise
IoT	Internet of things
ISO	International Organization for Standardization
ISOG	Information Security Officers Group
ITSG	International IT Supervisory Group
JABRACCC	Joint Anti-Bank Robbery Action and Cybercrime Coordinating Committee
JCSWG	Joint Cyber Security Working Group
KYC	Know-Your-Customer
NBI	National Bureau of Investigation
NCIAC	National Cybersecurity Inter-Agency Committee
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NSFI	National Strategy for Financial Inclusion
NTC	National Telecommunications Commission
OF	Open Finance
PNP	Philippine National Police
RBAP	Rural Bankers Association of the Philippines
SIEM	Security Incident and Event Management
SMS	Short Message Service
SOC	Security Operations Center
TIBER-EU	Threat Intelligence-based Ethical Red Teaming of the European Central Bank
TPSP	Third Party Service Providers
TTPs	Tactics, Techniques, and Procedures
USAID	United States Agency for International Development
VAPT	Vulnerability Assessment and Penetration Testing
WEF	World Economic Forum

Summary Table of FSCRP Goals, Priority Actions and Key Milestones

FSCRP Goal	Priority Action	Key Milestones					
		2024	2025	2026	2027	2028	2029
Goal 1 **Defined and coordinated incident response protocols and mechanisms**	**D1.** Establish baseline industry Incident Response Plan	Inventory/mapping of critical FIs/ interdependencies and identify cyber risk concentrations	Research and development and Plan Exposure Draft	Finalization and cascade to BSFIs			
	D2. Develop scenario-based incident response playbooks.	Develop playbook on Data Breach	Develop playbook on Supply Chain Attacks	Develop playbook on API Exploit	To be determined, depending on emerging threats		
	D3. Conduct progressive industry-wide cyber testing exercise regime.	Develop progressive industry-wide cyber testing exercise program and conduct pilot exercise	Industry Tabletop Exercise	Simulated scenario testing exercise	Annual testing to be conducted to include red-team test and scenario-based testing exercises		
	D4. Explore setting up of an industry Security Operations Center (SOC)		Conduct benchmarking study and research on industry SOC implementation of other jurisdictions	Consultation with industry associations and BSFIs Conduct feasibility study	Finalize recommendation		
Goal 2 **Active information sharing and collaboration**	**A1.** Expand and further enhance BAPCID as an industry sharing platform	Coordination with BAP and industry associations on the expansion strategy and address relevant concerns	Study potential linkages to other information sharing platforms	Enhance cybersecurity dashboards in ASTERisC for sharing in BAPCID platform			
		Oversee active engagement of BSFIs in BAPCID					
	A2. Strengthen and forge strategic partnerships in domestic and international fora	Engage industry associations on proposed initiative on fraud information sharing		Strengthen coordination with telco industry			
		Develop MOU for cyber coordination with CERT-PH and other relevant agencies					
		Continue active participation and engagement with domestic and international fora					
	A3. Support the enactment of cyber-related legislative initiatives	Passage of AFASA Bill and crafting of IRR		Passage of Amended Bank Secrecy Laws and crafting of IRR			

FSCRP Goal	Priority Action	Key Milestones					
		2024	2025	2026	2027	2028	2029
Goal 3 **Strong cybersecurity culture and awareness**	**S1.** Develop and implement cyber education program for BSFI Board and Senior Management	Consultation with industry associations and BSFIs	Current state assessment of BSFI cyber education program for Board & Sr. Mgt.	Development of cyber education program for Board and Sr. Mgt.	Implementation and monitoring		
	S2. Regularly conduct CISO/cyber forum and Annual Cybersecurity Summit	Continuing engagement					
	S3. Conduct cybersecurity roadshows for small and medium-sized FIs	Development and updating of materials for cybersecurity roadshows					
		Roadshows across regions to meet 100% of target BSFI participants					
	S4. Pursue holistic programs for cybersecurity skills and talent development	Research of best practices on cybersecurity skills development	Establishment of competency framework to guide the financial sector in building cyber-capabilities		Engagement of the academe and industry for collaborative cyber capacity building and education programs		
	S5. Mainstream cyber education and awareness programs for financial clients	Proposal for the creation of a dedicated website	Site design and development	Content development and management			
Goal 4 **Holistic cybersecurity best practices and standards**	**H1.** Complete policy reforms on digital security controls, API security, Cybersecurity Maturity Model Framework and Supply Chain Risk Management	Digital Security Controls and API Security	Cybersecurity Maturity Model Framework	Supply Chain Risk Management			
	H2. Explore establishment of an Industry Cyber Innovation/Research Hub		Research and study implementation in other countries	Conduct of feasibility and recommendations	Finalization and implementation of recommendations		
	H3. Conduct Benchmarking Exercises on Cyber Capabilities	Conduct research/ study visits relative to target area of cyber capability					

Endnotes

[1] **Banking Sector:** Includes all BSFIs and relevant Financial Market infrastructures within the BSP supervisory authority.

[2] **Money mules:** Refer to any person who use legitimate bank or financial accounts as channels to receive, transfer, or withdraw proceeds from crimes, offenses, or social engineering schemes.

[3] **Systemic risk:** As defined by the Financial Stability Board (FSB), the International Monetary Fund (IMF), and Bank for International Settlements (BIS), is the disruption to any part of the financial system that adversely affects the rest of the economy.

[4] MacBride, E. (2023, January 9). The dark web's criminal minds see Internet of Things as next big hacking prize. CNBC News. https://www.cnbc.com/2023/01/09/the-dark-webs-criminal-minds-see-iot-as-the-next-big-hacking-prize.html

[5] Definition by IBM, https://www.ibm.com/topics/quantum-computing

[6] Burns, R. (2023, February 22). The cybersecurity implications of quantum computing. Security InfoWatch. https://www.securityinfowatch.com/cybersecurity/information-security/managed-network-security/article/53012965/the-cybersecurity-implications-of-quantum-computing

[7] **The FinTech & RegTech Global Awards:** Organized by the Central Banking, a globally recognized organization that provides mainstream publications on central banking as well as organizes key events, meetings, and global awards aimed at advancing central banking and financial supervision agenda.

[8] **The Financial Sector Forum:** A voluntary inter-agency body comprised of the BSP, SEC, IC, and the Philippine Deposit Insurance Corporation (PDIC). It provides a platform for discussion of supervisory approaches and issues as well as emerging risks in the financial sector.

[9] **National Cybersecurity Talent Workforce Assessment Report of the Philippines:** 2022 Report by IBM with the support from the United States Agency for International Development (USAID).

[10] https://niccs.cisa.gov/workforce-development/nice-framework

BIBLIOGRAPHY

Australian Cyber Security Centre (ACSC). (n.d.). About the ACSC. https://www.cyber.gov.au/acsc

Bank Negara Malaysia. (n.d.). Management of Cyber Risks. https://www.bnm.gov.my/documents/20124/856377/cp03_001_box.pdf/0a5baa8d-a9f9-4bce-2d8a-b4e02665dc64?t=1585724984873

Department of Information and Communications Technology (2022). National CyberSecurity Plan 2022. https://www.pagba.com/wp-content/uploads/2019/05/Cyber-Security-Awareness-National-CyberSecurity-Plan-2022.pdf

European Central Bank. (n.d.). Cyber Resilience and Financial Market Infrastructures. https://www.ecb.europa.eu/paym/cyber-resilience/fmi/html/index.en.html

European Union Agency for Cybersecurity. (n.d.). European Cybersecurity Month. https://cybersecuritymonth.eu

IBM (2023). IBM X-Force Threat Intelligence Index 2023. https://www.ibm.com/reports/threat-intelligence

International Monetary Fund. Cyber Risk Surveillance: A Case Study of Singapore. https://www.elibrary.imf.org/configurable/content/journals$002f001$002f2020$002f028$002farticle-A001-en.xml?t:ac=journals%24002f001%24002f2020%24002f028%24002farticle-A

Monetary Authority of Singapore. (18 January 2021). MAS enhances guidelines to combat heightened cyber risks [Press release]. https://www.mas.gov.sg/news/media-releases/2021/mas-enhances-guidelines-to-combat-heightened-cyber-risks

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

U.S. Department of Homeland Security. (n.d.). National Cybersecurity Awareness Month. https://www.cisa.gov/cybersecurity-awareness-month

World Economic Forum. (11 Jan 2024). Global Cybersecurity Outlook 2024. https://www.weforum.org/publications/global-cybersecurity-outlook-2024/

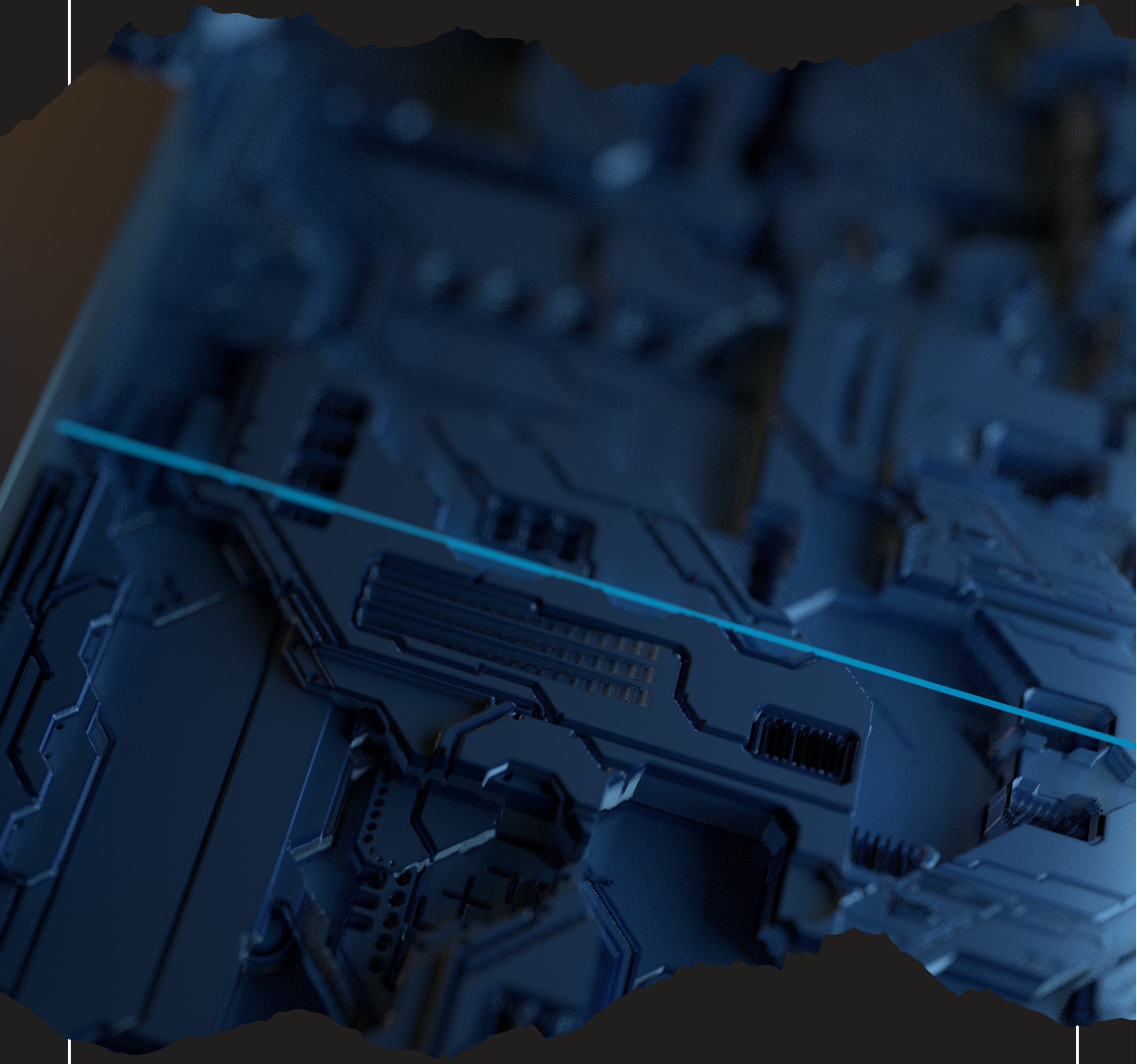
FINANCIAL SERVICES

CYBER RESILIENCE PLAN

2024 - 2029

BANGKO SENTRAL
NG PILIPINAS

TECHNOLOGY RISK AND INNOVATION SUPERVISION DEPARTMENT
2024



BANGKO SENTRAL NG PILIPINAS

www.bsp.gov.ph