TECHNICAL ASSISTANCE REPORT

PERU

Cybersecurity Strategy for the Financial Sector

February 2025

Prepared By

Tanai Khiaonarong (Mission Chief, MCM), Emran Islam (MCM), Terry Goh (MCM External Expert)

Authoring Department:

Monetary and Capital Markets Department

© 2025 International Monetary Fund

The contents of this document constitute technical advice provided by the staff of the International Monetary Fund to the authorities of Peru (the "CD recipient") in response to their request for technical assistance. Unless the CD recipient specifically objects to such disclosure, this document (in whole or in part) or summaries thereof may be disclosed by the IMF to the IMF Executive Director for Peru, to other IMF Executive Directors and members of their staff, as well as to other agencies or instrumentalities of the CD recipient, and upon their request, to World Bank staff, and other technical assistance providers and donors with legitimate interest (see Staff Operational Guidance on the Dissemination of Capacity Development Information). Publication or Disclosure of this report (in whole or in part) to parties outside the IMF other than agencies or instrumentalities of the CD recipient, World Bank staff, other technical assistance providers and donors with legitimate interest shall require the explicit consent of the CD recipient and the IMF's Monetary and Capital Markets Department.

The analysis and policy considerations expressed in this publication are those of the IMF's Monetary and Capital Markets Department.

International Monetary Fund, IMF Publications
P.O. Box 92780, Washington, DC 20090, U.S.A.
T. +(1) 202.623.7430 • F. +(1) 202.623.7201
publications@IMF.org
IMF.org/pubs

Contents

Figures

Tables

Annexes

Acronyms and Abbreviations

AI	Artificial Intelligence
ANPD	Autoridad Nacional de Protección de Datos Personales (National Authority of Personal Data Protection)
ASBANC	Asociación de Bancos del Perú (Association of Banks of Peru)
ASOMIF	Association of Microfinance Institutions of Peru
BCRP	Banco Central de Reserva del Perú (Central Reserve Bank of Perú)
CCE	Cámara de Compensación Electrónica S.A. (Automated Clearing House)
CERT	Computer Emergency Response Team
CIRT	Cyber Incident Response Team
CNSD	Centro Nacional de Seguridad Digital (National Center of Digital Security)
CPMI	Committee on Payments and Market Infrastructures
ECB	European Central Bank
FEPCMAC	Peruvian Credit Union Federation
FI	Financial Institutions
FIRE	Financial Incident Reporting Exchange
FMI	Financial Market Infrastructure
FSB	Financial Stability Board
FS-ISAC	Financial Services Information Sharing and Analysis Center
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IMF	International Monetary Fund
INDECOPI	Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (Competition and Consumer Protection Authority)
IOSCO	International Organization of Securities Commissions
ISO	International Organization for Standardization
ITU	International Telecommunications Union
LBTR	Sistema de Liquidación Bruta en Tiempo Real (Real-Time Gross Settlement System)
MEF	Ministerio de Economía y Finanzas, MEF (Ministry of Economy and Finance)
MFI	Microfinance Institutions
NIST	National Institute of Standards and Technology
RENIEC	Registro Nacional de Identificación y Estado Civil (National Registry of Identification and Civil Status)

SBS	Superintendencia de Banca, Seguros y AFP (Superintendency of Banking Insurance and Private Pension Fund Administrators)
SIM	Subscriber Identity Module
SLMV	Sistema de Liquidación Multibancaria de Valores (Payment Arrangements of the Securities Settlement System)
SMV	Superintendencia del Mercado de Valores (Superintendence of Securities Market)
TA	Technical Assistance
TLPT	Threat-Led Penetration Testing

Preface

At the request of the Superintendency of Banking Insurance and Private Pension Fund Administrators (SBS), a Technical Assistance (TA) mission from the Monetary and Capital Markets Department (MCM) of the International Monetary Fund (IMF) visited Lima, Peru during the period September 18 to October 1, 2024. Virtual meetings were also held during the period August 13 to 21, 2024. The purpose of the mission was to advise the authorities in developing a comprehensive cybersecurity strategy for the financial sector in Peru. Towards this objective, the mission:

- Reviewed the cyber posture of Peru to assess current capabilities and challenges.
- Met with financial sector authorities and external stakeholders to discuss developments and issues relating to the cyber resilience of the financial sector (Annex 1).
- Recommended actions to support the development of a comprehensive cybersecurity strategy for the financial sector in Peru and for the SBS.

The mission met with Mr. Sergio Espinosa Chiroque (Superintendent), and senior management and staff from the SBS, as well as representatives from the public and private sectors.

This TA report summarizes the findings and recommendations of the mission.

The mission wishes to express its appreciation to the SBS for their cooperation and for facilitating the meetings held with the various internal and external stakeholders.

Executive Summary

Cyber risk is recognized by authorities as posing a significant threat to the financial sector and overall financial stability in Peru. Cyberattacks targeting financial institutions (FIs) have included denial of service attacks, data breaches, phishing scams, malware, and ransomware. In 2023, a major cybersecurity incident involved a data breach at the national identity registry. The potential implications undermined public confidence and warranted authorities attention as an estimate of 14 million civil registration records have been digitized and interconnected with identity management, public health insurance, and banking systems. Compromised personal information led to a rise in cybercrime, according to authorities and industry sources. With further digitalization expected, authorities have plans to develop a comprehensive cybersecurity strategy for the financial sector. This report reviews the current situation and proposes recommendations (Table 1). This could be summarized as follows.

Element 1: Cybersecurity Strategy and Framework. Financial authorities—the banking, insurance, and pensions authority, central bank, securities regulator, and finance ministry—have a collective interest in the cyber resilience of the financial sector but there is currently no forum to discuss and coordinate on cybersecurity strategies. A high-level inter-agency committee is needed to drive sector-wide cybersecurity initiatives. Furthermore, collaboration and information sharing among FIs and authorities is lacking and there is no proper public-private forum on cyber resilience. A cyber resilience forum consisting of authorities and FIs is needed to foster collaboration and drive collective efforts to enhance the sector's cybersecurity.

Element 2: Governance. The banking authority has faced resource constraints with the continued digitalization of the financial sector and increase of cybersecurity risks of supervised entities. An increase of five additional staff are needed to support the onsite inspection of cybersecurity risks of supervised entities. A more comprehensive, detailed, and precise cybersecurity regulation was also suggested by public and private sector stakeholders.

Element 3: Risk and Control Assessment. While information on critical service providers used by FIs to determine concentration risks have been collected, mapping the financial system and cyber network still needs to be carried out. Cyber mapping would help provide a fuller picture of supervised firms and their information and communications technology (ICT) systems and can guide a supervisor's understanding of vulnerabilities in the financial system. Mapping financial and technology connections across the sector will help identify potential systemic risks from interconnectedness and concentrations in third-party service providers. The mapping of the financial sector network can also be used to estimate the impact of a cyber-attack on any of the nodes.

Element 4: Monitoring. While cyberattacks targeting FIs are documented, a comprehensive cyber threat landscape report is currently lacking. A Cyber Threat Landscape for the Peruvian Financial Sector Report could be considered to elaborate on the threats unique to the jurisdiction. This would assist authorities to foresee attack patterns and work with the FIs to better prepare for potential attacks through scenario development, building playbooks and exercising. While cybersecurity assessments could be conducted as part of general inspections or as a separate review, on-site inspections are prioritized for well-known cases as it is resource intensive and involve many supervisory responsibilities and recent focus has

shifted to more off-site supervision of the financial sector. An increase of onsite supervision of cybersecurity risks is needed with prioritization given to domestic systemically important banks. The lack of a red-team testing framework leaves the financial sector vulnerable to cyber threats. A comprehensive testing framework such as threat-led penetration testing is needed to help assess and enhance an FI's ability to detect, respond to, and recover from cyber incidents.

Element 5: Response. While a national Computer Emergency Response Team (CERT) for public institutions to enhance their cyber capabilities has been established by the National Center for Digital Security, no sectoral CERT is envisaged in their draft cybersecurity strategy for the country. Further, systemically important financial institutions and financial market infrastructures are not obligated to report cyber incidents to the national CERT for coordinated response. A CERT tailored to the needs of the financial sector should be set up to enhance the sector's ability to detect, respond to and mitigate cyber threats. It should also be integrated with the national CERT for broader coordination and to leverage on available expertise.

Element 6: Recovery. The first large-scale cyberattack simulation exercise was conducted in 2022. However, the securities regulator, capital market entities, and microfinance companies did not participate in the exercise, and the exercise was not designed to sufficiently test the communication and coordination between financial institutions in response to simulated cyber-attacks. A more comprehensive and inclusive approach should be taken in the design of future cyber exercises. A plan to conduct cross-sector and cross-border exercises is also needed to prepare the sector for cyber incidents with widespread operational and financial impact.

Element 7: Information Sharing. While a basic cyber information-sharing platform was introduced in 2022, it is only focused on collecting phishing information and information sharing lacked useful details. There is also currently no formal cyber incident reporting framework with a standardized format. A sector-wide threat intelligence information sharing platform and a standardized incident reporting framework is needed for effective and timely information sharing and coordinated responses. Public awareness campaigns by agencies and financial institutions are piecemeal and fragmented. A comprehensive cyber education and public awareness program, including a designated cyber month campaign, is needed.

Element 8: Continuous Learning. Developing a comprehensive cybersecurity strategy for the financial sector is a key priority and should be regularly reviewed and updated due to the rapidly evolving nature of cyber threats and vulnerabilities. With the emergence of generative artificial intelligence (AI) and quantum computing and applications in banking and finance, further innovation and future-proofing through studies and advisories issued to financial institutions on use, opportunities, and risks should be considered.

There could be challenges in implementing the cybersecurity strategy, which could be overcome with sector coordination and collective action. Prioritization and duration of each recommendation would need to be further discussed, decided, and sequenced by authorities and key stakeholders relative to their legal and institutional mandates and resource availability. They would also benefit from annual reviews, ongoing stakeholder consultations, and monitoring of the evolving cyber threat landscape. The implementation would require pooling resources and sector-wide coordination.

Recommendations

Table 1. Peru: Table of Recommendations

Recommendation	Time Frame 1/
Element 1: Cybersecurity Strategy and Framework	
Prioritize the establishment of a high-level inter-agency committee to drive national cybersecurity initiatives for the financial sector. (SBS, BCRP, SMV, MEF)	ST
Establish a public-private Cyber Resilience Forum that fosters active participation, collaboration and sharing with trusted stakeholders. (SBS, BCRP, SMV)	ST
Element 2: Governance	
Increase resources for cybersecurity risk supervision and oversight. (SBS)	ST
Enhance cybersecurity regulation. (SBS)	MT
Element 3: Risk and Control Assessment	
Map the financial system and cyber network. (SBS)	ST
Element 4: Monitoring	
Develop a Cyber Threat Landscape Report (SBS, BCRP, SMV)	MT
Increase onsite supervision of cybersecurity risks with a commensurate increase in capacity and resources. (SBS)	MT
Develop a cyber testing framework for controlled cyberattacks that simulates real-world threats. (SBS)	MT
Element 5: Response	
Establish a dedicated CERT for the financial sector (FinCERT) and integrate it with the national CERT. (SBS, BCRP, SMV, MEF)	MT
Element 6: Recovery	
Conduct comprehensive cyberattack simulation exercises, expand participation and develop a cross-authorities response framework for sector cyber resilience. (SBS)	MT
Element 7: Information Sharing	
Implement a sector-wide threat intelligence info-sharing platform and a standardized incident reporting framework. (SBS, BCRP, SMV)	ST
Implement a Comprehensive Cyber Education and Public Awareness Program, including a Cyber Month (SBS, BCRP, SMV, MEF)	ST
Element 8: Continuous Learning	
Conduct a formal survey to quantify cybersecurity skills gaps and develop a cyber competency roadmap for the financial sector. (SBS)	MT
Establish regular review for cybersecurity strategy and framework to be responsive to emerging threats. (SBS)	ST

Study and issue advisories to financial institutions on the use, opportunities and risks of generative artificial intelligence and quantum computing in the financial sector. (SBS)	MT

1/ Proposed responsible authorities—SBS, BCRP, SMV, MEF. Time Frame: Short-Term (ST): 1 year; Medium Term (MT): around 2 to 3 years; Long Term (LT): around 4 to 5 years.

I. Introduction

A. Background

1. Peruvian financial authorities have shown increasing interest in addressing cybersecurity challenges. Since 2021, the SBS has internally defined and developed a comprehensive cybersecurity roadmap under its leadership, limited to the scope of its mandate. This roadmap was built using the Global Cybersecurity Index methodology of the International Telecommunications Union (ITU). It includes five key pillars: developing the regulatory framework as an extension of the existing framework; promoting the corresponding technical and procedural implications; ensuring the establishment of the necessary organizational structures; fostering the development of human resource capacity; and encouraging cooperation. While cybersecurity supervision and oversight were not explicitly part of the roadmap, the SBS has focused its supervisory activities on information security and has developed dedicated cybersecurity supervisory tools. The roadmap has also been documented as a case study by the Alliance for Financial Inclusion (AFI), showcasing the SBS's approach. [1] The SBS has internally initiated, implemented, and monitored multiple actions aligned with this roadmap, which was planned for the period 2022-26.

2. As part of its strategy to promote cooperation, the SBS requested technical assistance (TA) from the IMF to develop a comprehensive cybersecurity strategy for the financial sector in Peru. The diagnosis of current challenges, supervisory capabilities, and capacity building needs are aimed to inform the strategy and enable the SBS to ensure a holistic approach towards strengthening the cyber resilience of the financial sector, safeguard the financial system, and foster sustained economic growth.

3. At the international level, Peru is categorized as having basic cybersecurity commitments. [2] Efforts to enhance the cyber resilience of the financial sector resonates with ongoing developments at the national level. Areas of relative strength include legal and organizational measures. Potential growth areas were identified in the areas of cooperation, technical, and capacity development measures. Peru lowest score was for technical measures, which reflects shortcomings in the implementation of technical capabilities through national and sector-specific agencies such as Cyber Incident Response Teams (CIRTs).

4. The Peru Financial Sector Assessment Program of 2018 did not cover a comprehensive review of the cybersecurity of the financial sector. The assessment noted that cyber risk was a part of operational risk-related regulations and all banks managed cyber risk under their operational risk

[1] See Alliance for Financial Inclusion (2021). Cybersecurity from the Perspective of the Financial Regulator and Supervisors in Peru, March.

[2] See ITU (2024) Global Cybersecurity Index 2024, 5th Edition. Peru is grouped under Tier 3 which is interpreted as establishing represents countries that obtained an overall score of at least 55/100 by demonstrating a basic cybersecurity commitment to government-driven actions that encompass evaluating, establishing or implementing certain generally accepted cybersecurity measures across a moderate number of pillars or indicators (page 133).

frameworks and incorporated cyber risk, business impact analysis and stress-testing exercises [3] Banks monitored cyber risk regularly, maintained organized cyber risk event databases, and have specific cyber risk insurance coverage. Some banks expected cyber risk standards to be made more explicit in regulations and aligned with international standards. The assessment also noted the lack of cyber-attack simulation exercises.

B. Cyber Threat Landscape

5. Cyber risk is recognized by authorities as posing a significant threat to the financial sector and overall financial stability in Peru. Although a comprehensive threat landscape is currently lacking, the banking authority has documented several cases involving cyberattacks targeting FIs, including denial of service attacks, data breaches, phishing scams, malware, ransomware, fake fingerprints, and technology disruptions. Based on internal records, 10 incidents occurred in 2023 and six incidents during 2024 (as of August) and involved banks, microfinance institutions, and e-money issuers. The most common and impactful threat to users in the financial sector is phishing. By stealing user credentials, cybercriminals perpetrate fraudulent activities that severely damage the sector's reputation.

6. In 2023, a major cybersecurity incident involved a data breach at the national identity registry. This involved the exposure of sensitive personal information, including fingerprints, at the National Registry of Identification and Civil Status (Registro Nacional de Identificación y Estado Civil, RENIEC). Information on the impact of the breach is not publicly available. The potential implications undermined public confidence and warranted authorities attention as an estimate of 14 million civil registration records (from a total of 60 million) maintained by municipal governments have been digitized.[4] Furthermore, RENIEC's Civil Registration and Vital Statistics systems are linked with identity management and public health insurance systems where 11 million workers (beneficiaries) could collect their payments from the nationwide network of branches of a state bank.

7. Compromised personal information led to a rise in cybercrime, according to authorities and industry sources. This involved the exploitation of user details to facilitate sophisticated impersonation tactics, such as the use of fake fingerprints for opening bank accounts. This also led to the loss of confidence by the financial industry in the cybersecurity of governmental services and their impact on the financial services sector. Impersonation attacks were also prevalent in the telecommunications sector during 2022 and 2023, leading to significant user losses.[5] In response, the SBS prohibited the sending of one-time passwords via short message services to mitigate these risks. To address this evolving threat landscape, the financial industry is investing heavily in advanced security measures and consumer education.

---

[3] See IMF (2018). Peru: Financial System Stability Assessment, Country Report No. 2018/238, July 25.

[4] See Centre of Excellence for Civil Registration and Vital Statistics (2020). Snapshot of Civil Registration and Vital Statistics Systems of Peru.

[5] These involved scams relating to subscriber identity module (SIM) swaps. So called SIM swap scams include methods where the fraud exploits a mobile phone service provider's ability to seamlessly port a phone number to a device containing a different SIM. This mobile number portability feature is normally used when a phone is lost or stolen, or a customer is switching service to a new phone. The scam begins with a fraudster gathering personal details about the victim, either by use of phishing emails, by buying them from organized criminals, directly socially engineering the victim, or by retrieval from online data breaches.

8. Peru's consumer protection body has also observed a rise in cybersecurity incidents and fraudulent transactions. Through its role in monitoring and handling of consumer complaints, cases in the banking sector have involved phishing, biometric data, spoofing, and vishing. This was evident in the post-COVID19 period and were largely targeted at vulnerable segments of society, including senior citizens, middle-aged persons, and those that are financial excluded. Cyber-attacks associated with impersonations, AI, supply chain are also areas of growing concern.

9. As the Peruvian financial landscape undergoes further digitalization, authorities and industry recognize that cybersecurity risks would also need to be monitored and addressed. This includes efforts to create interoperability and introduce open banking.[6] The central bank had led the development of a new fast payments system and conducted studies on central bank digital currencies.[7] The microfinance association also recognizes that such digital transformation of the financial landscape would require improved cyber preparedness of its members and their rural customers.

C. Cybersecurity Risk Supervision and Oversight Framework

10. The main authorities with responsibilities for cybersecurity risk supervision and oversight of the financial sector include:

- **Superintendency of Banking Insurance and Private Pension Fund Administrators (SBS).** The SBS oversees and ensures the stability, transparency, and soundness of the financial system. Its primary functions include regulating and supervising financial institutions such as banks, insurance companies, pension fund administrators, and other entities (municipal and rural savings and loan associations, cash management companies, finance companies, electronic money issuers, others). Around 109 entities are supervised by the SBS (of which 88 entities are onsite), including four domestic systemically important banks.

- **Central Reserve Bank of Perú (BCRP).** The BCRP is the central bank, with its primary mandate being to maintain monetary stability, manage international reserves, issue currency, and provide financial reports. The BCRP designates, regulates, and supervises three systemically important payment systems, including: (i) Sistema de Liquidación Bruta en Tiempo Real (Sistema LBTR)—a real-time gross settlement system; (ii) Cámara de Compensación Electrónica S.A (CCE)—an automated clearing house; and (iii) the Sistema de Liquidación Multibancaria de Valores (SLMV)—payment arrangements of the securities settlement system. In addition, it authorizes the organization and operation of clearing firms.

- **Superintendence of Securities Market (SMV).** The SMV is the regulatory authority responsible for overseeing the securities market in Peru. Around 81 entities are supervised by the SMV, where their activities are associated with clearing and settlement, stock exchange, fund management, mutual funds, investment, collective funds, securitization, pricing, and risk classification.

[6] See BCRP (2024). Assessing Peru's Retail Payments Interoperability Strategy: A Case Study, May.

[7] See BCRP (2023). CBDC: Promoting Digital Payments in Peru, March.

11. Additionally, multiple governmental authorities are involved in cybersecurity and have distinct roles and responsibilities as follows:

- **Ministry of Economy and Finance** (Ministerio de Economía y Finanzas, MEF) coordinates across the main financial sector authorities and has a common interest in cybersecurity issues that are relevant for capital markets, financial inclusion, and financial crisis management. The MEF has senior-level representation in the SMV and approves its financial budget.
- **National Authority of Personal Data Protection** (Autoridad Nacional de Protección de Datos Personales, ANPD) oversees the protection of personal data and ensures compliance with data protection laws.
- **National Digital Security Center** (Centro Nacional de Seguridad Digital, CNSD) focuses on the national cybersecurity strategy and coordinates responses to major cyber incidents.
- **Supervisory Agency for Private Investment in Telecommunications** (Organismo Supervisor de Inversión Privada en Telecomunicaciones, OSIPTEL) regulates and supervises telecommunications services, which are critical for cybersecurity in the financial sector.
- **Competition and Consumer Protection Authority** (Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual, INDECOPI) is involved in protecting consumers, which includes aspects related to cybersecurity.

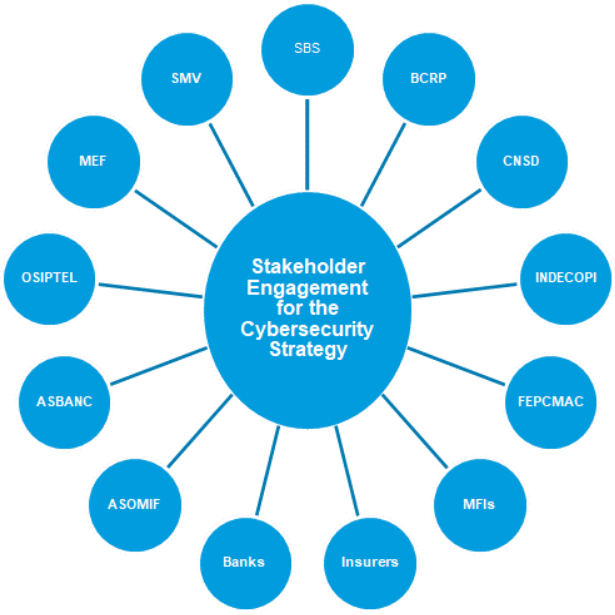
D. Methodology and Scope

12. The development of the cybersecurity strategy is guided by material developed by international standard-setting bodies and good practices from selected jurisdictions. The materials include:

- CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures (FMI) (June 2016).
- FSB Recommendations to Achieve Greater Convergence in Cyber Incident Reporting: Final Report (April 2023).
- IMF Cybersecurity Risk Supervision (2019).
- FSB Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices (October 2017).
- G7 Fundamental Elements of Cybersecurity for the Financial Sector

13. The mission took stock of the current situation from responses to a pre-mission questionnaire and meetings with key stakeholders (Figure 1). The questionnaire sought information on the cyber threat landscape, and cybersecurity risk supervision and oversight. The meetings with stakeholders further explored improvement opportunities and challenges associated with cybersecurity regulation and supervision; onsite and offsite supervision of cyber risk; threat intelligence and information sharing; testing frameworks; cyber response and recovery; cyber incident reporting; and cyber crisis simulations and exercises. The findings from the stock taking and meetings helped inform the development of the cybersecurity strategy for the financial sector.

Figure 1. Stakeholder Engagement for the Cybersecurity Strategy



Source: IMF staff

Notes: See acronyms and abbreviations for the full name of organizations.

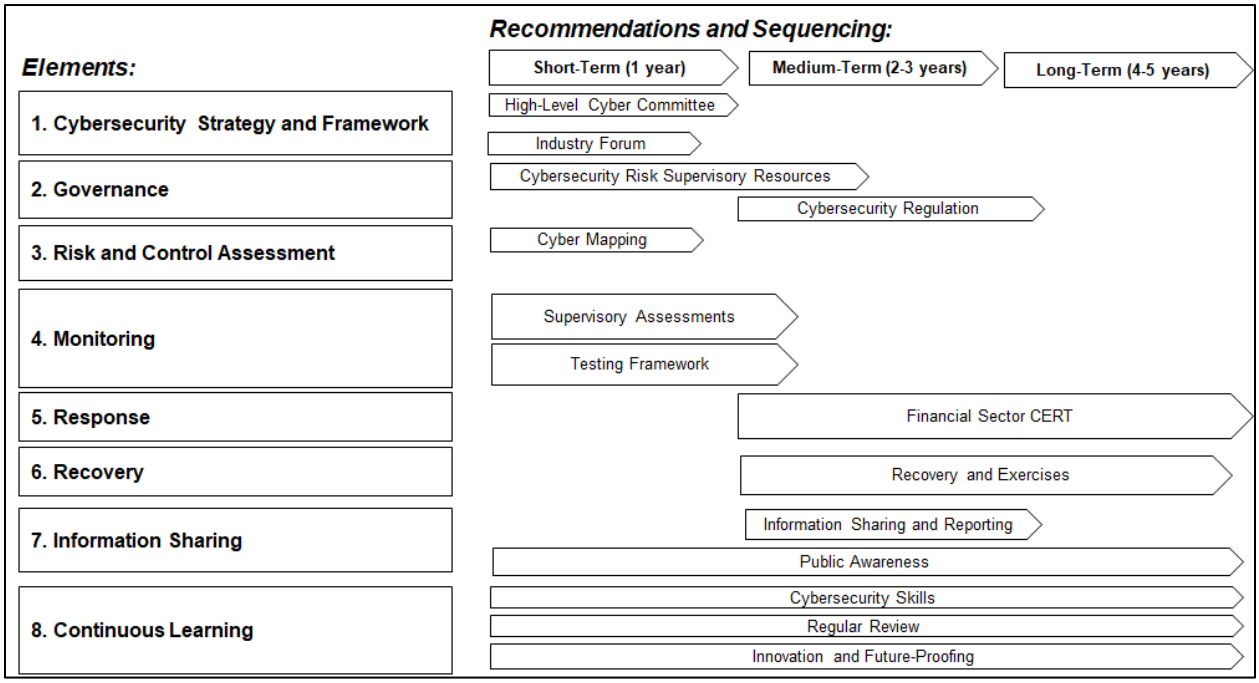
14. The cybersecurity strategy includes eight elements. Following discussions with the SBS, the mission applied the G7 Fundamental Elements of Cybersecurity for the Financial Sector which covers: (i) cybersecurity strategy and framework, (ii) governance, (iii) risk and control assessment, (iv) monitoring, (v) response, (vi) recovery, (vii) information sharing, and (viii) continuous learning (Annex 2). Each element is not intended to be mutually exclusive of other elements and could be interrelated for the purpose of this report. For example, there could be cross-cutting issues between the elements of risk and control assessment, monitoring, and recovery.

E. Next Steps

15. The SBS is committed to implementing the IMF's recommendations to enhance the cybersecurity resilience of Peru's financial sector. SBS will work diligently to ensure these recommendations are effectively integrated, fostering a collaborative environment with all relevant authorities and stakeholders. By prioritizing continuous improvement and innovation, SBS aims to strengthen the sector's defenses against emerging cyber threats, ensuring stability and security for the financial system.

16. A high-level overview of the elements and recommendations, where there are interrelationships, is provided in Figure 2. As next steps, prioritization and duration of each recommendation would need to be further discussed, decided, and sequenced by authorities and key stakeholders relative to their legal and institutional mandates and resource availability. They would also benefit from annual reviews, ongoing stakeholder consultations, and monitoring of the evolving cyber threat landscape.

Figure 2. Cybersecurity Strategy: Key Elements and Roadmap



Source: IMF staff

17. The scope of the mission did not cover the following: (i) the internal strategy for improving the cybersecurity risk management of the SBS; (ii) the strengthening of cyber resilience of systemically important FMIs; (iii) the developmental and operational aspects of establishing a financial sector CERT; and (iv) oversight and supervision of FMIs by the BCRP.

II. Element 1: Cybersecurity Strategy and Framework

A. High-Level Cyber Committee

Current situation

18. The SBS, SMV, BCRP and MEF take an interest in cyber resilience of the financial sector but lack a forum to coordinate and discuss national cybersecurity initiatives. The current lack of such a unified forum has led to the under-discussion and under-development of various critical sector-wide cyber initiatives. These include fundamental aspects like CERT implementation, information-sharing platforms, and formal sector-wide incident coordination.

19. There is a lack of consensus among the financial authorities and finance ministry to assume leadership and ownership of essential initiatives such as a financial sector CERT. No agency has stepped forward to lead due to potential concerns over expanding the agencies' core mandates and the substantial resources, costs, and effort required to manage and sustain such initiatives. As a result, there has been no clear assignment of responsibility, leading to fragmentation in critical cybersecurity functions and diminishing the overall effectiveness of the financial sector's resilience efforts. Without a designated lead agency or co-leading agencies, these initiatives risk being inconsistently implemented, further reducing the sector's cybersecurity effectiveness.

20. Given that financial stability is a common concern for the SBS, BCRP, SMV and MEF, inter-agency cooperation in cyber security for the sector is crucial. In the CPMI-IOSCO report, "A Compilation of Authorities' Experience with Cooperation" it was shown that collaboration among authorities is widely practiced. For decades, central banks, market regulators, and other bodies have consistently demonstrated the benefits of cooperation through various means, including informal interactions, formal agreements, and active participation in standard-setting bodies.[8] FIs and FMIs supervised by the three authorities are highly interconnected and this underscores the importance of coordinated oversight and collaboration among authorities.[9]

Recommendation

21. Prioritize the establishment of a High-Level Inter-Agency Committee for Coordinating National Cybersecurity Initiatives in the financial sector.[10] To address the current gaps in coordination and responsibility, a high-level committee consisting of the SBS, BCRP, SMV and MEF

[8] CPMI-IOSCO (2019) Responsibility E: A compilation of authorities' experience with cooperation.

[9] For example, Responsibility E of the CPMI-IOSCO Principes for FMIs describes how authorities should cooperate with each other, both domestically and internationally, as appropriate, in promoting the safety and efficiency of FMIs.

[10] See IMF (2018) Report on Peru: Financial System Stability Assessment Report, 2018. It was noted that the current legal framework provides for interagency cooperation and recommended that a high-level coordinating committee should be formed to assist in preparing for and managing a systemic financial crisis. The stakeholders are currently evaluating implementation mechanisms, and the authorities may integrate cybersecurity crisis into this committee's scope.

should be established, with clear terms of reference defined and key initiatives identified. While these form the core members, other agencies such as the CNDS should also be invited to participate. The approach should foster a collaborative environment, ensuring that key national cybersecurity initiatives are effectively developed, implemented, and maintained, ultimately strengthening the cyber resilience of the financial sector.

22. For the high-level committee to be effective, it should comprise of senior officials, especially heads of these authorities, including their deputies where applicable. To enable the committee to fulfill its mandate effectively, it is crucial for authorities to discuss and allocate resources to establish a secretariat to provide support to the committee. The committee's mandate would be to coordinate and agree on key national cybersecurity initiatives tailored to the financial sector, including overseeing the establishment of a sector-specific CERT, developing information-sharing platforms, and coordinating sector-wide incident response efforts. The committee should involve CNDS in its discussion on relevant agenda topics, to ensure comprehensive coverage and integration.

23. The committee should first conduct a stock-take of existing cybersecurity capabilities and initiatives across various agencies. This would involve identifying platforms like information-sharing mechanisms that individual authorities already have. Structured discussions and workshops within the committee should facilitate consensus on the importance and ownership of key initiatives like the sectoral CERT, information-sharing platforms, and incident response mechanisms. These sessions should address concerns related to resources, costs, and responsibilities, encouraging members to share perspectives and negotiate compromises to achieve a unified approach focused on the collective benefit for the financial sector and national cybersecurity.

24. Based on the stock-take, the committee should designate lead or co-leading agencies for each major initiative or consider unifying all initiatives under one lead for cohesive management. A rotating leadership model for chairing the committee can ensure shared ownership and prevent overburdening a single agency. The committee should also coordinate with non-financial sector agencies, particularly those involved in national security and critical infrastructure, to integrate financial sector initiatives into broader national cybersecurity efforts. This includes aligning financial sector CERTs and information-sharing platforms with those in sectors like energy and telecommunications.

25. To address concerns regarding resources, costs, and effort, the committee should develop a clear framework for resource allocation. This could include potential shared funding models or cross-agency support systems. It should also establish regular review cycles to assess the effectiveness of the initiatives and adapt to evolving cyber threats and challenges.

B. Industry Forum

Current situation

26. The SBS, SMV and BCRP have stepped up on regulating and supervising cyber risks, but collaboration among FIs and regulators is still lacking. FIs are hesitant to share cyber incidents or vulnerabilities with their regulators due to fears of being perceived as having weak cyber risk management and attracting supervisory scrutiny. This lack of trust hinders effective information sharing,

which is crucial for identifying and mitigating cyber threats. Without a framework that encourages open communication, efforts to enhance cyber resilience across the sector are likely to fall short. The absence of such a framework also limits the effectiveness of sector-wide exercises and other collaborative initiatives.

27. There is currently no forum dedicated to facilitating collaboration between FIs and public authorities to drive collective action on cyber resilience. The SBS has set up an Information Security Sectoral Working Group consisting of a few key banks and the Association of Banks of Peru (ASBANC), to allow the dialogue on common cybersecurity and authentication challenges and to find solutions. The lack of formal structures, including terms of reference, objectives, and a meeting schedule, has raised concerns about the group's legitimacy, for instance with a with a legal firm requesting the SBS to clarify the working group's right to publish the forum's non-binding recommendations. Such uncertainty demonstrated the necessity to formalize its existence. There is also a Market- wide Business Continuity Working Group which conducts business continuity exercises, including cyber-attack scenarios, but its scope does not address cyber-specific needs or initiatives.

28. Implementing a public-private partnership model is important for enhancing the sector's cyber resilience, as regulations and supervision alone cannot address these challenges. Establishing such a forum will promote meaningful collaboration and leadership, encouraging continuous dialogue and supporting various joint cyber initiatives. By bringing stakeholders together, the forum will ensure strategic guidance, drive executive-level engagement, and facilitate the successful implementation of sector-wide strategies.

29. Given the rapidly evolving threat landscape, establishing the forum should be a deliberate and immediate priority, rather than relying on gradual development over time. Regions such as the UK, USA, and EU have established forums like the Cross Market Operational Resilience Group (CMORG), the Financial Services Sector Coordinating Council (FSSCC), and the Euro Cyber Resilience Board (ECRB). These forums play a key role in coordinating sector-wide efforts, allowing stakeholders to collaborate on critical issues like threat intelligence sharing and joint cyber exercises. Establishing such a forum in Peru is imperative to safeguard the financial sector's resilience against increasing cyber risks.

Recommendation

30. Establish a public-private Cyber Resilience Forum that fosters active participation, collaboration and sharing experiences with trusted stakeholders. This forum will serve as a pivotal platform for fostering cooperation between FIs and public authorities. Its primary role should be to enhance sector-wide cyber resilience through strategic dialogue, collective problem-solving, and coordinated action. It should bring together senior representatives from key stakeholders, including high-level executives from major FIs, relevant government officials, and cybersecurity experts. This is to help ensure that the forum has the authority and expertise to tackle pressing cyber threats and coordinate comprehensive responses.

31. To implement this recommendation effectively, it is crucial to build trust through open and transparent communication between the financial regulator and FIs. Regular updates on regulatory changes, cyber threats, and collaborative efforts can foster trust. Highlighting the mutual benefits of the Cyber Resilience Forum, involving FI representatives in decision-making processes, and organizing

regular meetings, workshops, and training sessions are essential. Establishing feedback mechanisms to address FIs' concerns and suggestions, recognizing and rewarding active participants, and assuring the confidentiality of sensitive information shared within the forum will further enhance trust.

32. Defining the membership and leadership structure is another key action step. This involves including senior representatives from major FIs and relevant government agencies as core members, with the gradual inclusion of private sector cybersecurity experts. Appointing a chairperson or co-chairpersons from the SBS, BCRP or SMV, supported by a steering committee comprising representatives from both public and private sectors, is essential. Ensuring that members are senior executives or officials with decision-making authority will enable them to drive initiatives and allocate resources effectively.

33. To ensure the effectiveness of the forum, establish clear terms of reference, agendas, and priorities to enhance cyber resilience, information sharing, and sector-wide initiatives. Define operational procedures, including meeting frequency and decision-making processes, and set key agenda items such as threat landscape reviews and joint strategy development. Support the forum with a dedicated secretariat, sufficient resources, and staffing, and encourage participation through recognition programs, training, and awareness initiatives. Regularly monitor and evaluate the forum's effectiveness based on participation, initiative impact, and sector resilience improvements.

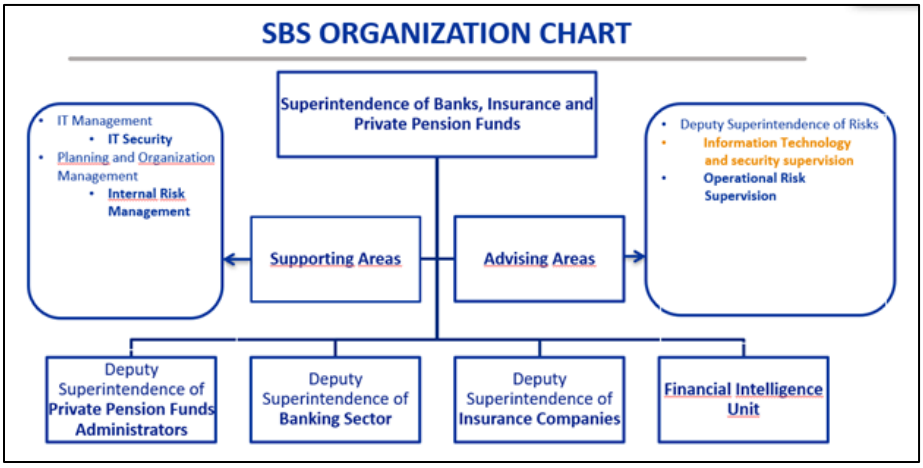
III. Element 2: Governance

A. Cybersecurity Risk Supervisory Resources

Current situation

34. SBS cybersecurity and operational risk supervision responsibilities are grouped under the Deputy Superintendent of Risks. This includes: (i) the Department of Information Systems and Security Supervision and (ii) the Department of Operational Risk Supervision (Figure 3). Both departments report to the Deputy Superintendent for Risks, which then reports to the Superintendent of Banks, Insurance and Private Pension Funds. The Department of Information Systems and Security Supervision is staffed with one department head, 15 supervisors, and two interns. Responsibilities include supervising information security and cybersecurity and ensuring the reliability of data in regulatory reports. Around 4 staff work full time in developing cybersecurity tools for off-site supervision, and 4 staff on information security supervision. Most staff are system engineers with expertise in information security and technology supervision.

Figure 3. Organization Chart of the SBS



Source: SBS

35. SBS faces resources constraints with the continued digitalization of the financial sector, which has increased the cybersecurity risks of supervised entities. While the SBS has financial autonomy, the level of available resources has constrained the speed and scope of regulatory activities, including cybersecurity supervision. SBS staff who work on information technology and security supervision have multiple responsibilities in addition to cybersecurity, including data reliability supervision and contribute to the work on the resolution of troubled FIs led by other departments within the SBS. While good progress has been made in improving the off-site supervision of cybersecurity risks, onsite supervision has been lacking relative to the number of entities supervised by the SBS, including the systemically important banks. Such resource constraints impact the ability of the SBS to expand its

supervisory and oversight capabilities or respond swiftly to emerging threats, as described in the previous section.

Recommendation

36. Increase resources for cybersecurity risk supervision as part of ongoing reorganization. Based on discussions with the authorities, five additional staff are needed to complement work in the Department of Information Systems and Security Supervision. The assessment of resource needs would need to consider factors such as emerging risks, technological advancements, and regulatory developments to ensure that adequate resources are allocated to fulfill regulatory responsibilities effectively. The additional resources should be considered in the context of supporting the onsite inspection of cybersecurity risks of supervised entities, particularly for domestic systemically important banks.

37. To be effective, authorities need to ensure that supervisors have the necessary experience and expertise to conduct effective cyber risk supervision. To assess a firm's cyber risk profile and cybersecurity risk control maturity level, adequate technical skills and an appropriate number of resources are needed. As skills gaps exist, filling these staffing gaps should be a key concern of authorities, given the impact cyber threats can have for financial stability. The combination of generalist supervisory skills (with an operational risk management focus) complemented with technical specialists have proven to be an effective solution. For specialized skills, the SBS could consider upskilling staff with competencies in cybersecurity and data sciences in addition to the recruitment of new employees with relevant skill sets. Hiring, training, and retention of specialists should be a key element of the strategy.

B. Cybersecurity Regulation

Current situation

38. The regulatory architecture governing the cybersecurity of FIs is structured around several key regulations and frameworks. These regulations collectively form the regulatory framework that ensures FIs adhere to robust cybersecurity practices, integrating them into broader risk management and business continuity strategies. Table 2 provides a list of the major regulations and circulars related to operational and cybersecurity risks issued by the SBS.

Table 2. Peru: Regulatory Framework for Cybersecurity Risks for the Financial Sector

Date	Regulation
2021	Information Security and Cybersecurity Regulation (Regulation 504-2021-SBS) (Last Update: June 2024)
2020	Business Continuity Management Regulation (Regulation 877-2020-SBS)
2019	Operational Risk Management (Regulation 2116-2009-SBS)
2017	Criteria for Recording Operational Loss Events (Circular G-191-2017)
2017	Corporate Governance and Integral Risk Management (Regulation 272-2017-SBS)
2015	Key Risk Indicators for Business Continuity Management (Circular G-180-2015)
2013	Credit and Debit Card Regulation (Regulation 6523-2013-SBS) (Last update: June 2024)
2012	New Products or Significant Changes (Circular G-165-2012)

2009	Operational Risk Management (Regulation 2116-2009-SBS)
2009	Requirement of Effective Capital for Operational Risk (Regulation 2115-2009-SBS)

39. Cybersecurity regulation is principle-based, setting out the requirements that FIs must meet without specifying the exact methods to achieve compliance. This approach provides flexibility in how institutions can implement and adhere to these requirements. The regulation on information security and cybersecurity was developed under the regulatory framework of risk management and more specifically under operational risk management regulation. The three main regulations, include:

- **The Information Security and Cybersecurity Regulation of 2021** establishes cybersecurity requirements for supervised entities and is being enhanced. This regulation contains guidelines and good practices applicable to information security management based on the National Institute of Standards and Technology (NIST) and ISO/IEC standards. The regulation includes provisions on services provided by third-party service providers, use of cloud services, and significant data processing services. Additionally, authorities expect to issue new circulars under this regulation, covering information sharing on cyber threats, reporting of cybersecurity incidents, and setting minimum evaluations for information security and cybersecurity management systems.

- **The Business Continuity Management Regulation of 2020** contains minimum standards for business continuity management. The regulation includes an obligation for financial institutions to report certain events that cause a significant interruption to their operations. A list of controls that a financial entity must implement in its business continuity management is also included.

- **The Operational Risk Management Regulation of 2009** establishes that financial institutions must have comprehensive risk management policies that are appropriate for their size and the complexity of their operations and services.

40. There are no current plans to issue regulations specifically on artificial intelligence. Regulations on model risk (053-2023-SBS) are, however, issued and authorities are planning to issue a new regulation on the principles for risk data aggregation.

41. Existing cybersecurity regulations have been difficult to interpret and implement in practice, according to industry stakeholders. Industry sources suggested that the setting of minimum standards for all financial institutions could help set a baseline for their cybersecurity, while higher standards could be considered for financial institutions in proportion to their higher risk profile. While the proportionality principle has been established in the regulatory regime for the different types of financial institutions, the principles could also be made more explicit in the existing cybersecurity regulations. Other potential areas for improvement include standardizing incident reporting, clarifying information requirements in the notification of cybersecurity incidents, and guidance on the quantification of risks for the purpose of cybersecurity risk insurance. Cybersecurity risks and operational risks should be further distinguished and clarified in regulation with the aim of ensuring that the regulation remains fit-for-purpose and receives greater attention and commitment by senior management and the Board of all financial institutions.

42. A more comprehensive, detailed, and precise cybersecurity regulation was welcomed. With further improvements, industry stakeholders view that this would help facilitate with efforts to ensure

regulatory compliance, consumer protection, enforcement, and sanctioning of financial institutions, if warranted. Industry sources also welcomed the opportunity to provide comments and suggestions on improving the existing cybersecurity regulation, although such feedback may not be binding.

43. Another emerging concern is the rise of identity theft related to the affiliation of merchants with payment processors. Existing cybersecurity regulations do not cover payment processors. According to authorities, there is no specific cybersecurity requirements and it is out of scope of SBS regulation.

Recommendation

44. Enhance cybersecurity regulations with guidelines. The SBS should continuously improve existing cybersecurity regulations.[11] Although all firms face cybersecurity risk, smaller and lower-capacity firms should focus on strengthening cyber hygiene, whereas the largest and most globally connected firms and key system nodes should be subject to heightened standards. Regulation should be in place to make cybersecurity requirements enforceable and to allow the use of supervisory actions where needed.

45. Cybersecurity regulation requirements should be applicable to supervised firms in a manner proportionate to their risk. While the Information Security and Cybersecurity Regulation of 2021 (Article 4) establishes the proportionality principles, industry sources suggest that the regulation lacked details. Requirements setting out the range of cybersecurity risk management controls should apply to all supervised firms, but increased complexity and systemic importance should be reflected in the maturity of controls. Regulation should also emphasize continuous improvement.

46. Based on the IMF Cyber Risk Supervisory Toolbox, the following topics should form the baseline of an effective regulation for all supervised firms:

- Governance and oversight
- Technology and cyber risk management
- IT services management
- Cybersecurity operations
- Response and recovery
- Scanning, testing, exercising, and remediation
- Independent assurance
- Outsourcing and technology service provider management

[11] This could involve benchmarking against international practices. See IMF Cyber Risk Supervisory Toolbox (unpublished). FSB (2017). Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices, October. Financial Stability Institute (2023). Banks' Cyber Security—A Second Generation of Regulatory Approaches, June.

IV.Element 3: Risk and Control Assessment

A. Cyber Mapping

Current Situation

47. SBS has collected information on critical service providers by entity and determined their concentration. This has helped provide a preliminary analysis of critical services. Authorities have also been involved in a project to test the cyber resilience of certain critical services relevant to the payment system with international assistance. Efforts to map the financial system and cyber network have not been done, however. Industry sources suggest that such cyber mapping could be useful in identifying interdependencies, for example between banks and insurance firms, and preparing contingency plans, as necessary. This would also help with coordination with other governmental agencies at the national level.

Recommendation

48. Conduct cyber mapping.[12] A full picture of supervised firms and their ICT systems will underpin a supervisor's understanding of vulnerabilities in the financial system. There are two distinct steps to this process: (i) firm level and (ii) sector wide. An in-depth understanding of a firm's ICT systems is the first step in this process. This step should build on supervisors' general knowledge of their supervised firms' business models, management of ICT risks, and importance for the financial sector. The second step is to consolidate firm-specific financial and technical connections to form a systemwide view—a financial sector network map that combines financial connections between systemic firms and their respective ICT connections. Added to this should be the identification of key technology systems in use by each supervised firm (whether they are in-house or delivered by third parties), as the usage of similar ICT systems can make supervised firms vulnerable to the same cyber-attack techniques. Knowledge of both financial and technical connections will help the supervisor to conduct firm-level supervisory risk assessments (for example, operational risk assessments, including ICT risk).

49. Mapping financial and technology connections across the sector will help identify potential systemic risks from interconnectedness and concentrations in third-party service providers. Assessing interconnectedness of the financial system network is essential for understanding how a shock to one supervised firm/utility/service provider can spread to others, potentially leading to a cascade of liquidity shortage, write-downs, and defaults. Identification of key nodes in the financial system—for example, the payment and settlement system, FIs that carry out key services such as clearing and the technology systems underpinning them—should be done to understand cyber risk on a systemwide basis. The mapping of the financial sector network can be used to estimate the impact of a cyber-attack on any of the nodes. The cyber map will also assist in identifying potential concentration risks in third-party service providers and protection mechanisms for assets.

[12] See IMF (2019). Cybersecurity Risk Supervision, Departmental Paper No. 19/15, for an illustration of the main steps and tools for cyber mapping.

V. Element 4: Monitoring

A. Cyber Threat Landscape Report

Current Situation

50. SBS collects and documents cases involving cyberattacks targeting FIs. However, a comprehensive cyber threat landscape report is currently lacking in Peru. Authorities could improve their overall analysis of the threat landscape by combining the different sources of information and developing a cyber threat landscape report that is updated annually. Based on international experiences, such reports could be a Generic Threat Landscape Report or a report that is tailored for the financial sector.[13]

Recommendation

51. Develop a Cyber Threat Landscape for the Peruvian Financial Sector Report. The report could elaborate on the specific threat landscape of the Peruvian financial system, taking into consideration threats unique to the jurisdiction. The report could consider key financial market participants and their critical functions, including (wholesale and retail) banks, broker, dealers, FMIs, and other critical third parties, the different threat actors (including their tactics, techniques, and procedures) targeting these entities, and the common vulnerabilities. By better understanding the threat landscape, the authorities would be well placed to foresee attack patterns and work with the financial institutions to better prepare for potential attacks through scenario development, building playbooks and exercising.

B. Supervisory Assessments

Current situation

52. Information security and cybersecurity are integral parts of the supervisory review process for FIs. Supervisory activities encompass both on-site and off-site reviews to ensure comprehensive oversight. Cybersecurity assessments could be conducted as part of general inspections or as a separate review. On-site inspections are prioritized for well-known cases as it is resource intensive and involve many supervisory responsibilities. Off-site supervision provides a wider assessment of the financial sector.

53. For on-site activities, the scheduling of inspections is based on identified cases where the supervision team has identified weaknesses in security or management. Additionally, this includes when a FI is applying for authorization to use the standard method of operational risk capital requirement. This authorization requires the FI to demonstrate good management practices for operational risk, business continuity, and information security. The scope of each revision is defined case by case. On

[13] For example, see the European Union Agency for Cybersecurity Threat Landscape 2024 and the Nordic Financial CERT 2024 Cyber Threat Landscape for the Nordic Financial Sector.

average, the SBS conducts 10 inspections where the scope of assessment is information security or cybersecurity.

54. For off-site activities, assessments are focused on specific topics to evaluate certain security domains across companies. Examples of recent reviews include the level of protection of credit and debit card information, security practices in mobile and web application development, and the black box assessment of vulnerabilities in mobile applications. Authorities have plans to assess the capabilities of incident response, security operation center capabilities, and cybersecurity program. A survey tool to improve the data collection process is being designed.

55. FIs are rated on their information security management practices on an annual basis. This score is integrated into the operational risk management rating. This is weighted and consolidated with other domains of supervision such as credit risk, solvency, and others. Any finding from on-site or off-site supervisions would impact the internal rating for information security. Depending on its importance, this could also impact the global internal score.

56. Onsite inspections related to information security or cybersecurity risks are conducted with a moderate level of intrusiveness. Only documentary evidence is required, and if the documents are confidential, they are reviewed solely during meetings with authorized personnel. Additionally, if it is necessary to validate highly technical aspects, independent third-party reviews could be required, and the resulting report must be submitted to the SBS.

57. Supervisory manuals reference various standards depending on the supervision objective. SBS use a tool (called Teammate) to record guidelines that are used for regular inspections. This includes the evaluation of security measures implemented for compliance with card standards (based on PCI and EMV standards), information security management, and security in operations and communications. Additionally, visits that involve the authorization of capital requirements by the alternative standard method based on operational risk use an Excel spreadsheet to collect specific information requirements for each security topic. This includes policies and organization for information security management, asset management (information and IT), control activities, personnel security, physical and environmental security, communications and operations security, logical security, security in the development or acquisition of information systems, and management of information security incidents. Such visits typically take between three to five weeks. In 2021, additional supervisory guidelines were issued for internal use only by supervisors, incorporating key standards such as the ISO 27000 series and the NIST Cybersecurity Framework (NIST CSF). However, these updated guidelines were not used due to the shift towards more off-site activities.

58. The supervisory process applies the proportionality principle through three distinct regimes that are based on the type of license held by an entity. Such categorization ensures that the supervisory process is tailored to their specific needs and risks, enhancing the effectiveness of oversight while maintaining proportionality. The three regimes include:

- **Simplified Regime.** This regime is applied to small entities. Requirements focus on basic and general security requirements to ensure a foundational level of protection.

- **General Regime.** This regime is for entities that need to implement comprehensive measures related to information security, authentication, security in third party providers, and cybersecurity. It includes more detailed requirements to address various aspects of security and cybersecurity.

- **Reinforced Regime.** This regime is applied to entities with significant market concentration and demands additional information security measures beyond those required in the General Regime.

59. FIs are required to have a comprehensive cybersecurity risk management process to address cyber risk as part of operational risk. This is subject to verification by the SBS. Companies authorized to use the Alternative Standard Method to determine operational risk capital requirements are required to hold additional capital to cover operational risk if they do not have adequate security practices. FIs are not required to set aside specific provisions for future cyber losses.

60. FIs are also required to include cyber-attack scenarios as part of their business continuity plans. A cyberattack simulation exercise was conducted involving the financial sector, insurance companies, pension fund administrators (AFPs), and key financial authorities in 2022. This exercise aimed to enhance preparedness and response strategies for significant cyber incidents.

61. The SBS could trigger supervisory measures in the event of shortcomings in information security or cybersecurity risk management within institutions. In recent years, supervisory actions have focused on evaluating vulnerabilities in mobile applications, requiring independent assessments for web and mobile platforms, verifying compliance with Payment Card Industry (PCI) standards, and assessing FIs' capabilities to detect and respond to phishing scams. Additionally, the SBS issued specific directives requiring institutions to take corrective actions in cases of information leaks or activities related to fraud. These measures ensure that institutions address and mitigate risks associated with information security and cybersecurity effectively.

Recommendation

62. Increase onsite supervision of cybersecurity risks with a commensurate increase in capacity and resources. Domestic systemically important banks should be prioritized given their higher risk profile and concentration risk. Cybersecurity risk should be assessed as part of the supervisory review process. Due to its large potential impact on a firm’s viability, cyber risk is an important subcategory of operational risk. Cybersecurity risk assessments are often undertaken within the operational risk assessment as part of the ICT risk assessment. Cybersecurity risk is relevant to the assessment of a firm’s governance, strategy, business model, and risks to capital. Cyber and ICT risks are typically considered material, as ICT systems form the backbone of almost all banking processes and distribution channels, support automated control environments on which core banking data is based, and are the key enablers of firms’ strategy.

C. Testing Framework

Current situation

63. FIs are required to conduct vulnerability scans and penetration tests when introducing new products or making changes to systems, but not on a regular basis. The SBS plans to make

their regular testing a requirement in the next update of the Regulations. However, there are no plans for FIs to perform Red team tests.

64. SBS also conducts security reviews on financial services mobile applications offered by FIs through its own laboratory, but they are limited in scope and purpose. The SBS conducts security reviews on mobile applications offered by FIs through its own laboratory. The personnel responsible for these tests are proficient in software development, trained by the ITU, and equipped with a manual for conducting tests and interpreting results. The scope of the tests is a subset of the Open Worldwide Application Security Project top ten mobile security framework, which is part of the recommendations of the ITU. As a supervisory tool, these reviews are not intended as a testing service for the industry nor as a certification, and the results—whether positive or negative—are fully shared with the FIs. For sustainability purposes, authorities could consider involving specialized third-party experts for future application security assessments.[14]

65. The financial sector also lacks a structured cyber testing framework that can help assess and enhance an FI's ability to detect, respond to, and recover from cyber incidents. The existing validation methods used by SBS rely heavily on self-assessments, audits, and onsite inspections, which provide limited insights into the actual resilience of FIs against cyber threats as they do not simulate real-world attacks.

66. The absence of such a comprehensive red-team testing framework creates a gap in cyber oversight of the financial sector. Without intrusive and realistic testing methodologies, the SBS has a constrained view of the effectiveness of cybersecurity policies and controls implemented by FIs. This gap makes it challenging to accurately assess preparedness and identify vulnerabilities that could be exploited by malicious actors. Having a testing framework will enable FIs to conduct a range of controlled and sophisticated tests such as red teaming, purple teaming, and gold teaming exercises.

67. A well-designed testing framework, such as a Threat-Led Penetration Testing (TLPT), also known as Red Team Testing, will provide deeper insights into the resilience of the sector. Such tests should evolve and adapt to the latest threat intelligence to help ensure that FIs are more prepared for sophisticated cyberattacks. For example, CPMI-IOSCO highlights the need to leverage cyber threat intelligence to design tests that simulate advanced threats and extreme scenarios. Examples of international best practices are shown in Annex 3.

Recommendation

68. SBS could consider involving specialized third-party experts for application security assessments in the future should it continue with its security laboratory program. This would help strengthen the approach if applications they have tested are later compromised in a cyberattack.

69. Prioritize vulnerability assessments and standarad penetration tests while developing a long-term cyber testing framework to simulate real-world threats through controlled cyberattacks.

[14] For example, authorities could further consider whether such security assessments could be considered as part of the work on vulnerability analysis that could be done under a financial sector CERT. See World Bank (2024) Digital First Responders: The Role of Computer Security Incident Response Teams (CSIRTS) in Developing Countries,

SBS should initially focus on ensuring frequent and extensive vulnerability assessments and non-adversarial penetration tests (PTs) across financial institutions (FIs). While some FIs may already be ready to adopt Threat-Led Penetration Testing (TLPT), its broader implementation should account for the overall maturity of the industry. TLPT should be introduced gradually, with a focus on higher-risk FIs first, given the significant costs and complexity involved. This approach ensures a balanced rollout while allowing institutions to build readiness over time.

70. The TLPT framework should incorporate various methodologies, including red, purple, and gold team exercises, and be informed by real-time threat intelligence. A structured TLPT program can evaluate the resilience of FIs against sophisticated cyber threats, drawing on established models like EU-TIBER and UK CBEST, and include a certification system for service providers to ensure quality.

71. To implement this effectively, form a working group within the Cyber Resilience Forum, including FIs, authorities, and experts, to design the framework and address sector-specific challenges. Partner with threat intelligence providers to integrate current threat landscapes into testing scenarios. Roll out the framework in stages, starting with systemically important FIs and gradually expanding to smaller entities. BCRP should also apply these guidelines to FMIs.

72. Design a TLPT framework outlining objectives, scope, and methodologies, ensuring it is intelligence-driven and focused on realistic scenarios. Create a certification process for external TLPT service providers to meet industry standards. Establish a dedicated team to oversee TLPT activities, ensuring consistent execution and proper addressing of findings. Develop a secure platform for sharing anonymized insights from TLPT exercises, promoting sector-wide resilience.

73. Use results from the cyber testing framework and TLPT exercises to enhance supervisory assessments of FIs' cyber resilience. This can be achieved by establishing feedback mechanisms to help FIs address identified gaps. Regularly review and update the framework to keep pace with the evolving cyber threat landscape.

VI.Element 5: Response

A. Financial Sector CERT

Current situation

74. CNDS has established a national CERT primarily to serve public institutions and no sectoral CERTs are envisaged in its draft cybersecurity strategy. The lack of guidance from CNDS for a financial sector CERT is also a growing concern for the SBS, SMV and BCRP. A national CERT safeguards a country's cybersecurity but lacks the specialized expertise needed for sectors like finance. The financial sector's interconnected and complex environment faces unique cyber threats, requiring faster responses and different regulatory considerations. A sectoral CERT for finance (FinCERT) can develop tailored threat intelligence, provide sector-specific incident response, and work closely with FIs and regulators. This ensures proactive and reactive cybersecurity measures are taken to address vulnerabilities unique to financial systems that a general CERT might not consider.

75. A major challenge contributing to the lack of FinCERT progress is that the SBS, BCRP and SMV do not see themselves as being responsible for leading such an initiative. As noted earlier, this hesitation stems from concerns over the costs, resource allocation, expertise required, and whether a CERT ownership would be within their mandate. Consequently, there has been no consensus or clear assignment of responsibility, leaving the financial sector without the specialized CERT it needs to effectively manage cyber risks. Moreover, the authorities have not conducted any studies to determine the scope of services and associated costs of operating a FinCERT, making it difficult to assess the feasibility and requirements for its implementation.[15]

76. FIs are not required to report cyber incidents to the national CERT, leading to a lack of integration between the financial sector and the national CERT. This gap hinders the sharing of critical threat intelligence, best practices, and coordinated responses to cross-sector incidents. Consequently, cybersecurity practices within the financial sector can become fragmented or inconsistent, weakening overall cybersecurity in Peru. Ensuring FinCERT's linkage with the national CERT is essential for enhancing the financial sector's resilience against cyber threats, integrating sector-specific needs into the broader national strategy, and improving overall cybersecurity posture.

Recommendation

77. Establish FinCERT and integrate it with the national CERT. This should be a key priority on the high-level committee's agenda. FinCERT should aim to provide specialized support in threat intelligence, incident response, vulnerability management, and situational awareness to the finance sector. It should also be tailored to the specific needs of the financial industry, ensuring that cybersecurity resilience is enhanced within the sector. To augment its effectiveness, FinCERT should be integrated with

[15] See World Bank (2024) Digital First Responders: The Role of Computer Security Incident Response Teams (CSIRTS) in Developing Countries, which provides rough estimates for the establishment of a national CSIRT at different levels of service offerings.

the national CERT to facilitate effective collaboration on broader cybersecurity threats and initiatives, leveraging shared resources and intelligence to bolster national and sectoral defenses.

78. Key actions include forming a FinCERT Project Task Force with representatives from relevant authorities to define roles, responsibilities, and protocols aligned with financial sector needs. A review of the legal and regulatory framework will ensure FinCERT can mandate reporting, enforce standards, and collaborate effectively. Funding should be secured, possibly through public-private partnerships, and Standard Operating Procedures (SOPs) developed to integrate business continuity and risk management. A pilot program will test the CERT with select institutions before full implementation.

79. Simultaneously, establish formal communication channels between FinCERT and the national CERT for seamless information sharing and coordinated incident responses. Develop integration protocols for collaboration during incidents, threat intelligence sharing, and joint exercises, ensuring both CERTs can address sector-specific and cross-sector threats. Conduct regular coordination meetings to review initiatives and emerging threats, to promote continuous improvement.

VII. Element 6: Recovery

A. Recovery and Exercises

Current situation

80. The SBS requires FIs to integrate cyberattack scenarios into their business continuity plans as part of efforts to bolster their resilience against cyber incidents. This mandate, introduced in 2020, ensures that FIs are prepared for potential disruptions caused by cyber threats. These continuity plans outline response strategies, resilience measures, and recovery procedures.

81. The SBS' conducted a large-scale cyberattack simulation exercise in 2022 involving commercial banks, select non-bank FIs, ASBANC, SBS, MEF and the BCRP. By simulating significant cyber threats, the exercise aimed to identify and address gaps in response strategies and enhance overall resilience. However, the SMV, the stock exchange, and Cavali, which operates the central securities depository and securities settlement systems did not participate in the exercise. Capital market firms and microfinance companies were also not involved in the exercise.

82. The exercise did not sufficiently test the cyber response, communication and coordination within the sector. Stakeholders found the cyber exercise beneficial for enhancing individual preparedness to respond to major cyber incidents. However, they highlighted a lack of adequate communication and coordination between FIs during the simulated incident.

83. While the exercise was insightful and helped authorities understand their cyber responses better, there's still no formal framework for them to coordinate response to a cyber crisis. This gap highlights the need for a comprehensive response framework that can coordinate not only among financial authorities but also with international partners when dealing with cross-border cyber incidents. A Cross-Authorities Response & Coordination Framework would facilitate structured collaboration between the central bank, financial supervisory authorities, technical experts, and other government bodies in managing the business and technical consequences of a cyber incident.

84. No cross-sector and cross-border exercises are being planned. The SBS has held cyber information-sharing talks with foreign regulators from Colombia, Chile and Mexico, focusing on exercise planning, but not actual exercises themselves. Also, while cooperation with the telecommunications regulator is in place, it is only focused on authentication issues faced by financial service providers. Conducting exercises across different sectors and borders is important in preparing for cyber incidents with widespread financial impact. These exercises enhance communication and coordination among stakeholders, ensure effective response strategies, and promote shared practices and lessons learned.[16]

[16] For example, cross-border exercises like the G7 Cyber Expert Group's simulation, demonstrate the importance of coordination in the face of cyber threats. These exercises strengthen the ability of financial authorities to communicate and respond effectively to crises, ultimately bolstering the financial sector's resilience.
https://www.bankingsupervision.europa.eu/press/pr/date/2024/html/ssm.pr240423~0f5ed951ef.en.html

Recommendation

85. Conduct comprehensive cyberattack simulation exercises, expand participation and develop a Cross-Authorities Response Framework, to enhance financial sector cyber resilience. The comprehensive approach should involve testing cyber response, communication, and coordination within the key stakeholder in the sector. To this end, the SBS should develop a formal Cross-Authorities Response and Coordination Framework to enhance crisis response by ensuring better coordination between the SBS, BCRP, SMV and MEF. The framework should enable authorities to coordinate effectively with FIs, FMIs, technical experts, and international partners during cyber incidents. It should also facilitate swift and informed decision-making, allowing the sector to mitigate the impacts of cyber incidents on both business operations and financial stability.

86. Consider future simulation exercises that stress tests system-wide liquidity in scenarios where critical FIs and FMIs are severely disrupted. These tests should account for potential liquidity contagion across financial institutions. While individual banks could perform their own stress tests, a system-wide approach would address broader spillover effects and contagion risks that may not align with individual priorities.[17]

87. The SBS should also take a more inclusive approach to the simulation exercises. This includes expanding the scope of participants to involve all relevant stakeholders, such as SMV, Cavali, capital market firms, and microfinance companies. This will allow communication and coordination arising from the interconnections and interdependencies among FIs, FMIs and authorities to be exercised.

88. The SBS should plan to conduct cross-sector and cross-border exercises to prepare for cyber incidents with widespread operational and financial impact. To make progress in cross-sector and cross-border exercises, the SBS can build on their existing efforts by taking a few key steps. Firstly, they can expand their existing cyber information-sharing meetings with foreign regulators to include actual exercises, not just planning. This will help them prepare for cyber incidents with widespread impact. Additionally, the SBS can broaden their cooperation with the telecommunications regulator to address a wider range of issues, beyond just authentication problems faced by financial service providers.

[17] For example, see Khiaonarong, T., K. Korpinen., and E. Islam (2025). Using Simulations for Cyber Stress Testing Exercises, IMF Working Paper No. 2025/085.

VIII. Element 7: Information Sharing

A. Information Sharing and Reporting

Current situation

89. The SBS gathers information on cybersecurity incidents primarily from reports submitted by FIs. The reports are provided when there are significant losses or theft of data, internal or external fraud, reputational damage, or operational disruptions. On average, it receives between 5 to 10 such incident reports annually. The reporting frequency and supervisory actions depend on the nature of the incident, and a forensic report must be provided to the SBS.

90. The SBS also maintains membership in the Financial Services Information Sharing and Analysis Center (FS-ISAC) for access to global threat intelligence. Additionally, the SBS collaborates with peer supervisors in other countries through memoranda of understanding, focusing on the exchange of information about banks with a presence in Peru and the home jurisdiction, within a home-host regulatory framework. By analyzing both incident reports and external threat data, the SBS identifies emerging risks and trends within the financial sector.

91. In June 2023, the SBS introduced a basic information-sharing platform, primarily focused on collecting phishing event data reported by FIs. Though the SBS intends to broaden the scope to include threats like ransomware and denial-of-service attacks, the platform is currently restricted to sharing event information without important details. Some FIs have also provided feedback indicating that they do not find the platform useful, as the information sharing is not real-time and the platform does not issue alerts.

92. There is a lack of comprehensive, sector-wide threat intelligence and information-sharing platform for the financial sector. Existing platforms are fragmented, e.g. the SBS' platform is limited to phishing and does not share important incident details, while ASBANC's privately operated information-sharing platform includes some but not all banks, excludes other FIs, and members do not actively share information. Some FIs are members of FS-ISAC, but their participation is minimal, with little active engagement in sharing critical cyber threat intelligence. While global platforms like FS-ISAC are valuable, they often lack the specific local context needed for timely responses to threats affecting the domestic market.

93. The SBS requires FIs to report incidents like data loss, fraud, and operational disruptions, but has yet to implement a formal cyber incident reporting framework with a standardized format. Cyber incidents are currently captured under the SBS' broader business continuity regulations but do not fully address the specifics of cyber incidents. Implementing a standardized incident reporting framework will enhance the effectiveness of incident data sharing, supporting a more robust information-sharing ecosystem and ensuring timely and coordinated responses among FIs and the SBS during cyber events. It will also benefit from aligning with the global FSB Recommendations to Achieve Greater Convergence in Cyber Incident Reporting and the design of a coordinated CIRR approach.

94. A sector-wide cyber threat info-sharing platform would enable more comprehensive sharing of incident information. Developing an effective threat intelligence platform requires systematic planning to ensure comprehensive coverage of all cyber threats and to foster active participation from all stakeholders. In the mission's onsite meetings with the different stakeholders, they expressed the need for a sector-wide cyber threat info-sharing platform to enhance collaboration, improve response times, and ensure a unified approach to tackling cyber threats across the sector. Without a strategic approach, the existing two platforms will remain constrained in its coverage and participation to facilitate real-time threat intelligence sharing across the financial sector.[18]

Recommendation

95. Implement a sector-wide threat intelligence info-sharing platform and a standardized incident reporting framework for effective and timely information sharing and coordinated responses. This initiative should start with a thorough assessment of the strengths and weaknesses of both the SBS' and ASBANC's existing platforms. The evaluation should aim to integrate the most effective features from each, ensuring comprehensive coverage of all cyber threats. A detailed analysis will determine whether to enhance one of the existing platforms, merge the two, or develop an entirely new solution. Establishing clear protocols for classifying and categorizing data will ensure the platform meets the specific needs of the financial sector. Encouraging active participation from FIs through incentives, recognition programs, and training will foster a culture of trust and collaboration, facilitating a robust threat intelligence framework.

96. To enhance the platform's capabilities, integrate it with the national CERT and international threat intelligence networks through formal data-sharing agreements. This will expand access to national and global threat intelligence, complementing sector efforts with broader insights. Establishing clear communication channels between teams and systems enables real-time threat sharing, automated incident response, and enhanced situational awareness. By fostering seamless collaboration, FIs can identify and respond to threats more efficiently, creating a safer and more resilient financial ecosystem.

97. Incident reporting across the sector should be standardized by adopting globally recognized frameworks, like the FSB's FIRE standard. This will ensure consistent, structured incident reports, improving the flow of data for more effective analysis and response. A sector-wide incident reporting tool should be developed and seamlessly integrated with the enhanced info-sharing platform for real-time reporting.

[18] FSB (2020) Effective Practices for Cyber Incident Response and Recovery, Final Report, shows that effective organizations share information on significant cyber threat intelligence, cyber incidents, effective cyber security strategies and risk management practices through trusted information sharing platforms. Technical information, such as indicators of compromise or vulnerabilities exploited, are shared as soon as it is available with certain level of anonymity according to the confidentiality warranted.

B. Public Awareness

Current situation

98. Consumers in Peru are becoming increasingly vulnerable to cyber-attacks due to weaknesses in the country's cybersecurity defenses. Incidents such as DDOS, data breaches, phishing and scams have exposed the ease with which attackers can exploit consumers. Phishing remains the most common and impactful threat, as it allows cybercriminals to steal credentials and commit fraud, leading to severe financial and reputational damage.

99. Compounding these threats are emerging tactics such as AI-powered attacks and supply chain vulnerabilities. Cybercriminals are using artificial intelligence to automate sophisticated attacks that can bypass traditional security measures, and they are exploiting weaknesses in third-party vendors to infiltrate FIs. As noted earlier, the recent breach at the national ID registry, which exposed sensitive personal information like fingerprints, has further intensified consumer vulnerability, enabling criminals to engage in more sophisticated impersonation and fraud.

100. Despite ongoing efforts to educate the public on the safe use of digital services, the country's approach remains piecemeal. Individual FIs invest in security technologies and targeted consumer education, but these efforts fall short of addressing broader, systemic challenges. Furthermore, FIs' awareness campaigns focus solely on their own customers. MEF conducts quarterly public awareness campaigns that include safe digital service use, but the focus is financial inclusion for the unbanked population. Agencies like INDECOPI and the SBS also conduct public awareness initiatives, but stakeholders have indicated that these efforts are insufficient and more extensive education is needed. Furthermore, INDECOPI's campaign has a consumer protection focus.

101. Cyber awareness must extend beyond piecemeal campaigns and develop into a strategic, sustainable, and comprehensive framework. Unlike many countries, including the US, Europe, and Australia, where September is dedicated to collaborative cybersecurity awareness activities between the public and private sectors, Peru lacks such large regular campaigns. Without a coordinated and holistic strategy, significant risks persist, leaving gaps that cybercriminals can exploit, ultimately undermining public confidence in digital services.

Recommendation

102. Implement a Comprehensive Cyber Education and Public Awareness Program, including a Cyber Month.[19] This initiative should aim to enhance consumer knowledge about cyber risks and improve their ability to protect against cyber-enabled fraud, including AI-powered attacks. It should be a concerted effort involving all stakeholders, such as banks, other FIs and their associations, various government agencies, and financial authorities. The High-level Interagency Committee should take the leadership to facilitate and coordinate this sustainable campaign.

[19] Examples of national efforts on public awareness programs that involve the financial sector (including scams, ransomware, other cyber threats): UK's Cyber Aware Program, Singapore's Be Safe Online and Australia's Stay Smart Online.

103. The program should aim to educate consumers on how to recognize and avoid potential frauds and cyber threats. FIs should establish clear communication guidelines, including avoiding the use of links, to mitigate phishing risks. These initiatives should be ongoing and dynamic, with regular updates to address emerging cyber threats and stay ahead of evolving risk landscapes.

104. Additionally, to promote a culture of cybersecurity, the public and private sectors should collaborate to declare and launch regular cybersecurity awareness initiatives. This should be a sustained awareness effort, for example by declaring every September a cybersecurity month[2].[20] These recurring campaigns should feature a series of activities, events, and engagements across the country, aiming to educate and empower citizens, businesses, and organizations to prioritize cybersecurity and protect themselves against emerging threats.

[20] Many countries dedicate one month a year as a national cybersecurity month in addition to ongoing public awareness and education programs, including in the USA (September), Europe (September) and Australia (October).

IX.Element 8: Continuous Learning

A. Cybersecurity Skills

Current situation

105. There has not been any formal or comprehensive survey specifically addressing the shortage of cybersecurity skills in the financial sector of Peru. While cybersecurity is recognized as an important issue, concrete data on skills gaps is lacking. Although the development of cybersecurity capabilities was incorporated in the current cybersecurity roadmap for the financial sector, a survey explaining the need for coordinated efforts by relevant authorities and industry was not included. Efforts to develop a cyber competency roadmap does not appear to have been initiated by any authority or industry.

106. Despite the absence of formal data, authorities have observed several indicators of a potential skills shortage in the country. For example, the heads of cybersecurity of three of the four systemically important banks come from foreign countries (Colombia, Brazil, and Spain) and suggested a lack of local talent for high-level cybersecurity positions. Another observation was the movement of cybersecurity professionals who often develop their careers by alternating positions between different FIs, indicating a competitive job market for these skills. This competition for talent has had cascading effects as the hiring strategies of major banks have left smaller companies with a shortage of specialized personnel. This situation potentially exposes smaller FIs to greater cybersecurity risks, which could have broader implications for the sector's overall security posture.

107. Authorities have responded to these challenges with several initiatives, including training and education. The SBS has promoted various training events, of which some were promoted by the Information Security Sectoral Working Group with international collaboration. In recent years, cybersecurity undergraduate and postgraduate programs in local universities have also emerged in recent years. However, authorities are uncertain whether this training would fully cover the needs of the market and the financial services sector. While these efforts are encouraging, the lack of comprehensive data makes it difficult to assess their effectiveness. Authorities estimate that the financial sector may still face a significant shortfall in cybersecurity professionals, potentially in the hundreds, though exact figures are hard to determine without a formal survey.

108. While the SBS does not have extensive external programs to develop cybersecurity talent in the financial sector, it does provide some internal support for cybersecurity training. This includes covering costs for some international cybersecurity certifications for IT supervisors, allocating a shared annual training budget, and occasionally acquiring online training platforms for cybersecurity and IT subjects. However, these efforts are primarily focused on internal staff development and face some limitations in terms of budget and long-term sustainability. In case an international certification is obtained (Certified Information Systems Auditor and Certified Information Systems Security Professional) by a supervisor, annual fees to maintain certification need to be paid, which is not attractive unless supervisor has another income source that can support the investment.

109. Several private sector initiatives have been aimed to promote training, competition for cybersecurity skills upgrading in the financial sector. This includes workshops on various topics related to information security and cybersecurity (such as a course on assembly) organized by ASBANC. Some banks have also provided scholarships to cover university studies for eligible students in fields such as systems engineering but not on cybersecurity, while others offer cybersecurity programs online. Authorities are not aware of specific government-led programs, collaborations with universities for research, cybersecurity camps and competitions, or innovation labs in partnership with technology companies focused on cybersecurity in the financial sector.

Recommendation

110. Conduct a formal survey to quantify cybersecurity skills gaps and develop a cyber competency roadmap for the financial sector. This should include enhancing collaboration between FIs, universities, and regulators to align educational programs with industry needs. This would help develop the market for cyber qualifications, accreditation, and certification, to build overall capacity and address skills shortage to maintain the integrity and security of Peru's financial sector in an increasingly digital world. The development of a cyber competency roadmap would also help establish the different levels of essential skills for progress in cyber roles.

111. To further bolster cybersecurity capacity, implement a national cybersecurity training program tailored to the financial sector. Collaborate with educational institutions, private companies, and international partners to develop specialized courses and certifications. Establish centers of excellence for cybersecurity research and innovation to foster collaboration and drive advancements in cybersecurity. Related to the earlier recommendation, launch public awareness campaigns to educate the public and financial sector employees about cybersecurity best practices. Provide financial incentives for obtaining industry-recognized certifications to build a robust cybersecurity workforce.

B. Regular Review

Current situation

112. Developing a comprehensive cybersecurity strategy for the financial sector is a key priority for the SBS, and this technical assistance report provides crucial input in that effort. In 2021, the SBS, in partnership with the Alliance for Financial Inclusion, published a case study that outlined a cybersecurity roadmap for the financial sector and recommended the development of a tailored cybersecurity strategy, setting the stage for the SBS's current cybersecurity efforts. The insights and recommendations from this TA report will play a vital role in shaping the cybersecurity approach, informing key decisions, and ensuring the effective protection of the financial sector.

113. Besides developing a cybersecurity strategy that aligns with the recommendations in this report, the SBS should also conduct regular reviews and updates to its cybersecurity strategy. This is important due to the rapidly evolving nature of cyber threats and vulnerabilities. The G7's Fundamental Elements of Cybersecurity for the Financial Sector emphasizes the importance of continuous learning and evolution in cybersecurity frameworks to address shifting threat landscapes, technological advancements, and increased reliance on third-party service providers. Periodic reviews will

help maintain the effectiveness of cybersecurity measures, optimize resource allocation, address gaps, and incorporate lessons learned from past incidents.

Recommendation

114. Establish a regular review process to assess and update the cybersecurity strategy and framework. The objective should be to ensure that the cybersecurity strategy for the financial sector remains effective and responsive to emerging threats and the broader sectoral strategy involves multiple authorities. This established process should include annual reviews of the cybersecurity strategy and framework. Additionally, the SBS should engage with FIs, industry experts, and other relevant stakeholders to gather diverse insights and feedback. Consider external developments in related sectors, such as energy and telecommunications, that could impact the financial sector's cyber resilience.

115. To maintain its cybersecurity effectiveness, the SBS should prioritize continuous learning and improvement, leveraging on cross-cutting activities in the recommendations of this report. This includes conducting post-incident reviews, analyzing lessons learned, and refining its strategy accordingly. Additionally, the SBS should engage in collaboration and information sharing with industry peers, regulators, and specialized cybersecurity firms. Other key activities include cybersecurity exercises, simulations, and training programs; subscribing to threat intelligence feeds and industry publications; and attending conferences, workshops, and webinars.

116. Furthermore, the SBS should invest in its employees through regular security awareness training, mentorship programs, and knowledge sharing among team members. Staying abreast of emerging technologies and innovative cybersecurity solutions is also crucial. To achieve this, the SBS can engage with academic institutions and research centers, leveraging their cutting-edge expertise. By embracing continuous learning, the SBS enhances its cybersecurity posture, maintaining a proactive stance against evolving threats and fostering a culture of ongoing improvement and adaptability.

C. Innovation and Future-Proofing

Current situation

117. Peru faces cybersecurity threats that have increased in sophistication. As described in the cyber threat landscape, this has included cybersecurity incidents involving impersonations which was exasperated with the major data breach of the RENIEC in 2023. While the SBS has benefitted from having a computer laboratory staffed with qualified system engineers that have helped addressed mobile payment security and other challenges so far, they continue to be faced with evolving risks stemming from new and emerging technologies. For example, this could include the use of generative artificial intelligence (AI)[21] and quantum computing[22] in future cyber-attacks.

[21] See United States Department of the Treasury (2024). Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector, March.

[22] See Monetary Authority of Singapore (2024). Advisory on Addressing the Cybersecurity Risks Associated with Quantum, Circular No. MAS/TCRS/2024/01; and G7 Cyber Expert Group (2024) Statement on Panning for the Opportunities and Risks of Quantum Computing, September.

118. Feedback from stakeholders also suggests the need to prepare for the associated risks that could arise with the use of generative AI in the financial sector. Leading financial authorities in countries have proactively issued advisories on the safe use of generative AI. As part the effort to future-proof against these emerging cyber threats, funding support for regulated entities to defray manpower and technology costs in building capabilities in these areas has also been observed.[23]

Recommendation

119. Study and issue advisories to FIs on the use, opportunities and risks of generative AI and quantum computing in the financial sector. The studies could be in collaboration with the involvement of other agencies such as the CNSD, government bodies, ASBANC, private companies, and universities. Authorities could encourage financial institutions to consider taking important steps to address the emerging risks. This could aim at developing a better understanding of generative AI and quantum computing, the risks involved, and strategies for mitigating risks; assessing generative AI and quantum computing risks in their areas of responsibility; and developing a plan for mitigating generative AI and quantum technology risks. Furthermore, the SBS could provide guidelines on best practices for implementing AI and quantum technologies, ensuring that FIs are well-prepared to handle the evolving threat landscape. This proactive approach will help in safeguarding the financial sector against potential cyber threats and maintaining the integrity and security of financial systems.

120. Additionally, it is important for the SBS to keep tabs on and maintain control over these emerging risks. This involves continuous monitoring of technological advancements and cyber threat trends, updating advisories and regulations as necessary, and fostering a collaborative environment where FIs can share insights and best practices. The SBS should issue best practice guidelines when appropriate, ensuring alignment with technological advancements and sectoral readiness. By staying vigilant and adaptive, authorities can ensure that the financial sector remains resilient against the dynamic challenges posed by generative AI and quantum computing.

[23] The Monetary Authority of Singapore (MAS) has highlighted the potential impact of quantum computing on cybersecurity, urging financial institutions to adopt post-quantum cryptography (PQC) and quantum key distribution (QKD) technologies to mitigate these risks. Additionally, MAS has committed S$100 million to support financial institutions in building capabilities in quantum and AI technologies, which includes supporting manpower costs and technology solutions. Similarly, U.S. agencies such as the National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), and National Institute of Standards and Technology (NIST) have warned that cyber actors could leverage future quantum computing technology to break traditional non-quantum-resistant cryptographic algorithms.

Annex I. Agenda for the Meetings

Date	Topic
September 18	**Meeting with Banking, Insurance and Pension Funds Authority**
2pm-2:30pm	▪ Courtesy visit to SBS senior management
2:30pm-5pm	▪ Opening meeting ▪ **Superintendency of Banking, Insurance, and Pension Funds (SBS)** role and responsibilities in relation to cybersecurity ▪ Overview of banking, insurance, and pension in Peru ▪ Cybersecurity risk supervision and oversight framework for banks, insurance, and pensions in Peru
September 19	**Meeting with Automated Clearing House and National Cyber Security Agency**
10am-12pm	▪ **Peru's Automated Clearing House (CCE)** role and responsibilities in relation to cybersecurity ▪ Current threat landscape for retail payments ▪ Threat intelligence and information sharing, testing framework, cyber incident response and recovery, cyber incident reporting, cyber crisis simulation and exercises
2pm-5pm	▪ **National Center of Digital Security (CNSD)** role and responsibilities in relation to cybersecurity ▪ National Cyber Strategy and Cybersecurity Legislation ▪ Threat intelligence and information sharing, testing framework, cyber incident response and recovery, cyber incident reporting, cyber crisis simulation and exercises
September 20	**Meeting with Securities Regulator**
10am-12pm	▪ **Superintendencia del Mercado de Valores (SMV)** role and responsibilities in relation to cybersecurity ▪ Overview of securities markets and market infrastructures in Peru ▪ Current threat landscape and Cyber strategy of the SMV
2pm-5pm	▪ Cybersecurity oversight and supervisory framework for securities entities and market infrastructures in Peru ▪ Onsite and offsite supervision of cyber risk, threat intelligence and information sharing, testing framework, cyber incident response and recovery, cyber incident reporting, cyber crisis simulation and exercises
September 23	**Meeting with Central Bank, Telecommunications Authority, and Competition and Consumer Protection Authority**
10am-12pm	▪ **Banco Central de Reserva del Perú (BCRP)** role and responsibilities in relation to cybersecurity ▪ Overview of payments and market infrastructures in Peru ▪ Payment systems developments (including instant payments, interoperability and so on) ▪ Current threat landscape Cyber strategy of the central bank ▪ Cybersecurity oversight and supervisory framework for payments and market infrastructures in Peru
2pm-3pm	▪ **Supervisory Agency for Private Investment in Telecommunications (OSIPTEL)** role and responsibilities of the in relation to cybersecurity ▪ Current threat landscape

	▪ Threat intelligence and information sharing, testing framework, cyber incident response and recovery, cyber incident reporting, cyber crisis simulation and exercises
4pm-5pm	▪ **National Institute for the Defense of Free Competition and the Protection of Intellectual Property (INDECOPI)** role and responsibilities in relation to cybersecurity
September 24	**Meeting with Central Bank, Bank Association, and Microfinance Association**
10pm-12pm	▪ **BCRP** onsite and offsite supervision of cyber risk, threat intelligence and information sharing, testing framework, cyber incident response and recovery, cyber incident reporting, cyber crisis simulation and exercises
2pm-3pm	▪ **Association of Banks of Peru (ASBANC)** role and responsibilities in relation to cybersecurity ▪ Current threat landscape for the banks ▪ Threat intelligence and information sharing, testing framework, cyber incident response and recovery, cyber incident reporting, cyber crisis simulation and exercises
4pm-5pm	▪ **Association of Microfinance Institutions of Peru (ASOMIF)** role and responsibilities in relation to cybersecurity ▪ Current threat landscape for the Microfinance institutions ▪ Threat intelligence and information sharing, testing framework, cyber incident response and recovery, cyber incident reporting, cyber crisis simulation and exercises
September 25	**Meeting with FIs**
10am-12pm	▪ **BCP** cybersecurity risk management, threat intelligence and information sharing, testing framework, cyber incident response and recovery, cyber incident reporting, cyber crisis simulation and exercises.
3pm-4pm	▪ **CMAC Arequipa** cybersecurity risks management, threat intelligence and information sharing, testing framework, cyber incident response and recovery, cyber incident reporting, cyber crisis simulation and exercises.
4:15pm-5:15pm	▪ **Positiva Seguros y Reaseguros** cybersecurity risk management, threat intelligence and information sharing, testing framework, cyber incident response and recovery, cyber incident reporting, cyber crisis simulation and exercises.
September 26	**Meeting with FIs and Federation of Municipal Savings and Credit Banks**
10am-12pm	▪ **Banco de la Nación** cybersecurity risk management, threat intelligence and information sharing, testing framework, cyber incident response and recovery, cyber incident reporting, cyber crisis simulation and exercises.
2pm-3pm	▪ **Peruvian Federation of Municipal Savings and Credit Banks (FEPCMAC)** role and responsibilities in relation to cybersecurity ▪ Current threat landscape for the microfinance institutions ▪ Threat intelligence and information sharing, testing framework, cyber incident response and recovery, cyber incident reporting, cyber crisis simulation and exercises
September 27	**Meeting with Ministry of Economy and Finance**
10am-12pm	▪ **Ministry of Economy and Finance (MEF)** role and responsibilities in relation to cybersecurity
September 30	**Meeting with Banking, Insurance and Pension Funds Authority**
10am-12pm	▪ Discussion of preliminary findings and recommendations
October 1	**Meeting with Banking, Insurance and Pension Funds Authority**
10am-12pm	▪ Closing meeting with SBS senior management

Annex II. G7 Fundamental Elements of Cybersecurity for the Financial Sector

Increasing in sophistication, frequency, and persistence, cyber risks are growing more dangerous and diverse, threatening to disrupt our interconnected global financial systems and the institutions that operate and support those systems. To address these risks, the below non-binding, high-level fundamental elements are designed for financial sector private and public entities to tailor to their specific operational and threat landscape, role in the sector, and legal and regulatory requirements.

The elements serve as the building blocks upon which an entity can design and implement its cybersecurity strategy and operating framework, informed by its approach to risk management and culture. The elements also provide steps in a dynamic process through which the entity can systematically re-evaluate its cybersecurity strategy and framework as the operational and threat environment evolves. Public authorities within and across jurisdictions can use the elements as well to guide their public policy, regulatory, and supervisory efforts. Working together, informed by these elements, private and public entities and public authorities can help bolster the overall cybersecurity and resiliency of the international financial system.

Element 1: Cybersecurity Strategy and Framework. Establish and maintain a cybersecurity strategy and framework tailored to specific cyber risks and appropriately informed by international, national, and industry standards and guidelines.

The purpose of a cybersecurity strategy and framework is to specify how to identify, manage, and reduce cyber risks effectively in an integrated and comprehensive manner. Entities in the financial sector should establish cybersecurity strategies and frameworks tailored to their nature, size, complexity, risk profile, and culture. Informed by the cyber threat and vulnerability landscape, a jurisdiction can also establish sector-wide cybersecurity strategies and frameworks that outline how cooperation occurs between entities and public authorities in the financial sector, with sectors upon which the financial sector depends, and with other relevant jurisdictions.

Element 2: Governance. Define and facilitate performance of roles and responsibilities for personnel implementing, managing, and overseeing the effectiveness of the cybersecurity strategy and framework to ensure accountability; and provide adequate resources, appropriate authority, and access to the governing authority (e.g., board of directors or senior officials at public authorities).

Effective governance structures reinforce accountability by articulating clear responsibilities and lines of reporting and escalation. Effective governance also mediates competing objectives and fosters communication among operating units, information technology, risk, and control related activities. Consistent with their missions and strategies, boards of directors (or similar oversight bodies for public entities or authorities) should establish the cyber risk tolerance for their entities and oversee the design, implementation, and effectiveness of related cybersecurity programs.

Element 3: Risk and Control Assessment. Identify functions, activities, products, and services—including interconnections, dependencies, and third parties—prioritize their relative importance, and

assess their respective cyber risks. Identify and implement controls—including systems, policies, procedures, and training—to protect against and manage those risks within the tolerance set by the governing authority.

Ideally as part of an enterprise risk management program, entities should evaluate the inherent cyber risk (or the risk absent any compensating controls) presented by the people, processes, technology, and underlying data that support each identified function, activity, product, and service. Entities should then identify and assess the existence and effectiveness of controls to protect against the identified risk to arrive at the residual cyber risk. Protection mechanisms can include avoiding or eliminating risk by not engaging in an identified activity. They can also include mitigating the risk through controls or sharing or transferring the risk. In addition to evaluating an entity's own cyber risks from its functions, activities, products, and services, risk and control assessments should consider as appropriate any cyber risks the entity presents to others and the financial sector as a whole. Public authorities should map critical economic functions in their financial systems as part of their risk and control assessments to identify single points of failure and concentration risk. The sector's critical economic functions range from deposit taking, lending, and payments to trading, clearing, settlement, and custody.

Element 4: Monitoring. Establish systematic monitoring processes to rapidly detect cyber incidents and periodically evaluate the effectiveness of identified controls, including through network monitoring, testing, audits, and exercises.

Effective monitoring helps entities adhere to established risk tolerances and timely enhance or remediate weaknesses in existing controls. Testing and auditing protocols provide essential assurance mechanisms for entities and public authorities alike. Depending on the nature of an entity and its cyber risk profile and control environment, the testing and auditing functions should be appropriately independent from the personnel responsible for implementing and managing the cybersecurity program. Through examinations, on-site and other supervisory mechanisms, comparative analysis of entities' testing results, and joint public-private exercises, public authorities can better understand sector-wide cyber threats and vulnerabilities, as well as individual entities' relative risk profiles and capabilities.

Element 5: Response. Timely (a) assess the nature, scope, and impact of a cyber incident; (b) contain the incident and mitigate its impact; (c) notify internal and external stakeholders (such as law enforcement, regulators, and other public authorities, as well as shareholders, third-party service providers, and customers as appropriate); and (d) coordinate joint response activities as needed.

As part of their risk and control assessments, entities should implement incident response policies and other controls to facilitate effective incident response. Among other things, these controls should clearly address decision-making responsibilities, define escalation procedures, and establish processes for communicating with internal and external stakeholders. Exercising protocols within and among entities and public authorities contributes to more effective responses. Exercising also enables entities and public authorities to identify how potential decisions could affect each other's ability to maintain critical and other functions, services, and activities.

Element 6: Recovery. Resume operations responsibly, while allowing for continued remediation, including by (a) eliminating harmful remnants of the incident; (b) restoring systems and data to normal and confirming normal state; (c) identifying and mitigating all vulnerabilities that were exploited; (d)

remediating vulnerabilities to prevent similar incidents; and (e) communicating appropriately internally and externally.

Once operational stability and integrity are assured, prompt and effective recovery of operations should be based on prioritization of critical economic and other functions and in accordance with objectives set by the relevant public authorities. Maintaining trust and confidence in the financial sector significantly improves when entities and public authorities have the ability to mutually assist each other in the resumption and recovery of critical functions, processes, and activities. Therefore, before an incident occurs, establishing and testing contingency plans for essential activities and key processes, such as funding, can contribute to a faster and more effective recovery.

Element 7: Information Sharing. Engage in the timely sharing of reliable, actionable cybersecurity information with internal and external stakeholders (including entities and public authorities within and outside the financial sector) on threats, vulnerabilities, incidents, and responses to enhance defenses, limit damage, increase situational awareness, and broaden learning.

Sharing technical information, such as threat indicators or details on how vulnerabilities were exploited, allows entities to remain up-to-date in their defenses and learn about emerging methods used by attackers. Sharing broader insights among entities, between entities and public authorities, and among public authorities deepens collective understanding of how attackers may exploit sector-wide vulnerabilities that could potentially disrupt critical economic functions and endanger financial stability. Given its importance, entities and public authorities should identify and address impediments to information sharing.

Element 8: Continuous Learning. Review the cybersecurity strategy and framework regularly and when events warrant—including its governance, risk and control assessment, monitoring, response, recovery, and information sharing components—to address changes in cyber risks, allocate resources, identify and remediate gaps, and incorporate lessons learned.

Cyber threats and vulnerabilities evolve rapidly, as do best practices and technical standards to address them. The composition of the financial sector also changes over time, as new types of entities, products, and services emerge, and third-party service providers are increasingly relied upon. Entity-specific, as well as sector-wide, cybersecurity strategies and frameworks need periodic review and update to adapt to changes in the threat and control environment, enhance user awareness, and to effectively deploy resources. Other sectors, such as energy and telecommunications, present external dependencies; therefore, entities and public authorities should consider developments in these sectors as part of any review process.

Annex III. International Practices of Comprehensive Testing Framework

The CPMI-IOSCO's Cyber Resilience Guidance for FMIs emphasizes that a comprehensive testing program is crucial to validate the effectiveness of their cyber resilience frameworks regularly.[24] It should leverage cyber threat intelligence to design tests that simulate advanced threats and extreme scenarios. The program should include various methodologies such as vulnerability assessments, scenario-based testing, penetration tests, and red team exercises. These tests should involve both internal and external stakeholders, including business continuity and crisis response teams, to ensure robust operational resilience. The results should be used to continuously improve cyber resilience, with appropriate involvement and awareness of senior management and the board.

The European Central Bank (ECB) has developed the Threat Intelligence-Based Ethical Red Teaming (TIBER-EU) framework, which provides a structured approach for FIs to conduct controlled cyberattack simulations based on credible threat intelligence.[25] TIBER-EU helps institutions identify and address weaknesses in their people, processes, and technologies by emulating tactics used by real adversaries. This framework has been successfully adopted across various EU jurisdictions, enhancing the overall cyber resilience of the European financial sector. Source: ECB TIBER-EU Framework, 2018

The Bank of England has introduced the CBEST framework, which delivers intelligence-led penetration testing for the UK's most significant FIs.[26] CBEST combines threat intelligence from government and accredited providers to simulate sophisticated attacks, providing a realistic assessment of an institution's cyber defenses and response capabilities. This approach has significantly improved the understanding and management of cyber risks within the UK financial sector. Source: Bank of England CBEST Framework

[24] CPMI-IOSCO Guidance on cyber resilience for FMIs.

[25] ECB's TIBER-EU FRAMEWORK How to implement the European framework for Threat Intelligence-based Ethical Red Teaming

[26] CBEST Framework (Bank of England).