# HIGH-LEVEL SUMMARY 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)

 HLS/25/26

**High-Level Summary Technical Assistance Report**
Monetary and Capital Markets Department

# Peru: Cybersecurity Strategy for the Financial Sector

Prepared by Tanai Khiaonarong, Emran Islam (all MCM), and Terry Goh (MCM External Expert)

The *High-Level Summary Technical Assistance Report* series provides high-level summaries of the assistance provided to IMF capacity development recipients, describing the high-level objectives, findings, and recommendations.

ABSTRACT: Cyber risk is recognized by authorities as posing a significant threat to the financial sector and overall financial stability in Peru. With further digitalization expected, authorities have plans to develop a comprehensive cybersecurity strategy for the financial sector. Guided by the G7 Fundamental Elements of Cybersecurity for the Financial Sector, this covers: cybersecurity strategy and framework; governance; risk and control assessment; monitoring; response; recovery; information sharing; and continuous learning. There could be challenges in implementing the cybersecurity strategy, which could be overcome with sector coordination and collective action [88 words].

| JEL Classification Numbers: E4, E5, G2, K24 |
| --- |
| Keywords: Peru, cybersecurity, financial sector, strategy, supervision |



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

# Background

At the request of the Superintendency of Banking Insurance and Private Pension Fund Administrators (SBS), a technical assistance mission from the Monetary and Capital Markets Department of the International Monetary Fund 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. 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, and recommended actions to support the development of a comprehensive cybersecurity strategy for the financial sector.

# Summary of Findings

Financial authorities 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. The banking authority has faced resource constraints with the continued digitalization of the financial sector and increase of cybersecurity risks of supervised entities. While information on critical service providers used by financial institutions (FIs) to determine concentration risks have been collected, mapping of the financial system and cyber network and a comprehensive cyber threat landscape report are still needed. While a national Computer Emergency Response Team (CERT) for public institutions has been established by the National Center for Digital Security, no sectoral CERT is envisaged. While cyberattack simulation exercises were conducted, the exercise was not designed to sufficiently test the communication and coordination between financial institutions. While a basic cyber information-sharing platform exist, 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.

# Summary of Recommendations

The mission made 15 recommendations as follows: (i) prioritize the establishment of a high-level inter-agency committee to drive national cybersecurity initiatives for the financial sector; (ii) establish a public-private Cyber Resilience Forum; (iii) increase resources for cybersecurity risk supervision and oversight; (iv) enhance cybersecurity regulation; (v) map the financial system and cyber network; (vi) develop a Cyber Threat Landscape Report; (vii) increase onsite supervision of cybersecurity risks with a commensurate increase in capacity and resources; (viii) develop a cyber testing framework for controlled cyberattacks that simulates real-world threats; (ix) establish a dedicated CERT for the financial sector and integrate it with the national CERT; (x) conduct comprehensive cyberattack simulation exercises, expand participation and develop a cross-authorities response framework for sector cyber resilience; (xi) implement a sector-wide threat intelligence info-sharing platform and a standardized incident reporting framework; (xii) implement a Comprehensive Cyber Education and Public Awareness Program; (xiii) conduct a formal survey to quantify cybersecurity skills gaps and develop a cyber competency roadmap for the financial sector; (xiv) establish regular review for cybersecurity strategy and framework to be responsive to emerging threats; and (xv) study and issue advisories to financial institutions on the use, opportunities and risks of generative artificial intelligence and quantum computing in the financial sector.