INTERNATIONAL MONETARY FUND

IMF Country Report No. 22/340

MEXICO

FINANCIAL SECTOR ASSESSMENT PROGRAM

November 2022

TECHNICAL NOTE ON TECHNICAL NOTE ON CYBER RESILIENCE AND FINANCIAL STABILITY

This Technical Note on Technical Note on Cyber Resilience and Financial Stability for the Mexico FSAP was prepared by a staff team of the International Monetary Fund as background documentation for the periodic consultation with the member country. It is based on the information available at the time it was completed in October 2022.

Copies of this report are available to the public from

International Monetary Fund • Publication Services
PO Box 92780 • Washington, D.C. 20090
Telephone: (202) 623-7430 • Fax: (202) 623-7201
E-mail: publications@imf.org Web: http://www.imf.org
Price: $18.00 per printed copy

International Monetary Fund
Washington, D.C.

INTERNATIONAL MONETARY FUND

MEXICO

FINANCIAL SECTOR ASSESSMENT PROGRAM

October 25, 2022

TECHNICAL NOTE

CYBER RESILIENCE AND FINANCIAL STABILITY

Prepared By
Monetary and Capital Markets Department, IMF

This Technical Note was prepared by IMF staff in the context of the Financial Sector Assessment Program (FSAP) in Mexico. The note contains the technical analysis and detailed information underpinning the FSAP findings and recommendations. Further information on the FSAP program can be found at http://www.imf.org/external/np/fsap/fssa.aspx.

CONTENTS

Glossary ____ 4

EXECUTIVE SUMMARY ____ 6

INTRODUCTION ____ 11
A. Background: Cyber Risk as a Financial Stability Concern ____ 11
B. Review Scope: Banks, Nonbanks, and Financial Market Infrastructures ____ 12

STRATEGY AND GOVERNANCE ____ 13
A. Cyber Strategy ____ 13
B. Institutional Framework ____ 14
C. Governance Arrangements ____ 15
D. Coordination and Cooperation ____ 18
E. Resources ____ 19
F. Recommendations ____ 20

FINANCIAL SYSTEM AND CYBER MAPPING ____ 21
A. Cyber Map of the Financial System ____ 21
B. Outsourcing and Third-Party Risk ____ 22
C. Recommendations ____ 24

CYBER REGULATORY FRAMEWORK AND SUPERVISORY PRACTICES ____ 25
A. FMI Cyber Oversight ____ 25
B. Cyber Supervision ____ 29
C. Recommendations ____ 31

MONITORING, RESPONSE AND RECOVERY ____ 33
A. Monitoring ____ 33
B. Response and Recovery ____ 35
C. Recommendations ____ 36

INFORMATION SHARING AND INCIDENT REPORTING ____ 37
A. Information Sharing ____ 37
B. Incident Reporting ____ 37
C. Recommendations ____ 40

CYBER DETERRENCE _____ **40**

BOX

1. Responsibilities of DG-ISS and DG-OTR at CNBV _____ 17

FIGURES

1. Structure of Possible Financial Sector Cyber Map _____ 24
2. FMI Landscape _____ 26

TABLES

1. Recommendations on Cyber Resilience and Financial Stability _____ 9
2. Responsibility of Divisions in the Directorate of Cybersecurity at Banxico _____ 16
3. Cyber Incidents During 2020–2021 _____ 34
4. Cyber Incidents Reporting Regimes _____ 38

Glossary

ABM	*Asociación de Bancos de México* (Mexican Banking Association)
AMIB	Mexican Association of Brokerage Institutions
AMSOFIPO	Mexican Association of Popular Financial Companies
APT	Advanced Persistent Threat
BANCOMEXT	Banco Nacional de Comercio Exterior
Banxico	*Banco de México* (Central Bank)
BCBS	Basel Committee on Banking Supervision
CCP	Central Counterparty
CERT	Computer Emergency Response Team
CESF	*Consejo de Estabilidad del Sistema Financiero* (Financial System Stability Council)
CESI	Information Security Specialized Committee
CIDGE	Inter-Ministerial Commission for the Development of Electronic Government
CISO	Chief Information Security Officer
CNBV	*Comisión Nacional Bancaria y de Valores* (National Banking and Securities Commission)
CNSF	*Comisión Nacional de Seguros y Fianzas* (National Insurance and Sureties Commission)
CONCAMEX	Confederation of Savings and Loan Cooperatives of Mexico
CONDUSEF	*Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros* (National Commission for Financial Services Consumer Protection)
CONSAR	*Comisión Nacional del Sistema de Ahorro para el Retiro* (National Commission for Savings for Retirement)
CPMI	Committee on Payments and Market Infrastructures
CPSS	Committee on Payment and Settlement Systems
CSD	Central Securities Depository
CSP	Cloud Service Provider
FGR	General Attorney Office
FMI	Financial Market Infrastructure
FSB	Financial Stability Board
FS-ISAC	Financial Services Information Sharing and Analysis Center
GRI	Information Security Sensitive Incident Response Group
GTL	Generic Threat Landscape
ICT	Information and Communication Technology
IMF	International Monetary Fund
INAI	*Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales* (National Institute of Transparency, Access to Information and Protection of Personal Data)
IOSCO	International Organization of Securities Commissions
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology

OSSAT	European Central Bank's Operational Security Situational Awareness Secretariat
SHCP	*Secretaría de Hacienda y Crédito Público* (Ministry of Finance and Public Credit)
SPEI	Interbank Electronic Payment System
SWIFT	Society for Worldwide Interbank Financial Telecommunications
TTP	Tactics, Techniques and Procedures

EXECUTIVE SUMMARY[1]

Mexico's financial system is digitalizing rapidly, increasing exposure to cyber risk. As in other jurisdictions, internet and mobile banking users in Mexico have increased substantially, but cyber incidents have also surged in recent years. The tight interdependencies within its financial system, and beyond, make Mexico vulnerable to evolving cyber threats. Thus, the Financial System Stability Council (CESF) has recognized cyber as a risk with potential to impact financial stability.

Banco de México (Banxico) and Comisión Nacional Bancaria y de Valores (CNBV) have made significant progress in enhancing the cyber resilience of the financial sector, but further work and enhancements are needed. Each authority has within its organization a dedicated division in charge of promoting cybersecurity and cyber resilience in the financial sector. Formal agreements to improve coordination and cooperation within the financial sector in the field of cybersecurity are an excellent example of coordination and cooperation, in comparison to international peers. Banxico has developed a cybersecurity strategy. However, both authorities would benefit from an enhancement to the cyber strategy that specifies how to effectively identify, manage, and reduce cyber risk for the financial sector and the financial market infrastructures in an integrated and comprehensive manner at a systemic level.

Banxico should strengthen the cyber risk oversight of financial market infrastructures (FMIs). Although Banxico's supervision of participants that connect into the Interbank Electronic Payment System (SPEI) is strong, Banxico should set clear regulatory requirements for all the FMIs under its mandate, leveraging the CPMI-IOSCO guidance, thereby increasing the cyber resilience of the FMIs. In addition, intensive cyber training of overseers, combined with a structured, comprehensive cyber oversight approach and adequate tools, would increase the capabilities and effectiveness of the oversight function.

The payment system oversight function should be given adequate independence and resources to conduct thorough oversight of the SPEI system. Banxico applies three lines of defense model (i.e., operations, risk management, and internal audit) to operate the SPEI system, as well as secured transmission of information and accountability rules, benefiting from strong cybersecurity and operations units. But there is no formal oversight to conduct its own independent, continuous, and intensive oversight of SPEI as a systemically important payment system in the context of the CPMI/IOSCO principles. Granting adequate independence from the SPEI operators and resources will help the oversight division, within the Directorate General of Payment Systems and Market Infrastructures, to fulfill Banxico's mandate towards all payment systems, including SPEI.

Cyber risk regulation and supervisory practice need significant improvements. CNBV is encouraged to issue enforceable guidance or regulation to all its supervised financial entities on

[1] This Technical Note has been prepared by Emran Islam (IMF, Monetary and Capital Markets Department, Financial Supervision and Regulation Division). The FSAP thanks the authorities for the constructive dialogue and the many insights that they have shared.

cyber risk, not only for credit institutions and fintech.[2] CNBV should also implement a more structured, risk-based approach to cyber supervision, supported by adequate tools. Onsite inspections of financial entities have just started in April 2022, and offsite supervision would benefit from clear identification of possible risks, like transmission of information not well secured and the lack of accountability rules. Finally, the cyber supervision unit should be given sufficient resources to discharge its responsibilities and use a mix of different regulatory tools (e.g., use of independent auditors), thereby maximizing efficiency with its limited resources.

Banxico and CNBV would benefit from considering developing a cyber map of the financial system. While cyber mapping is an emerging field, it will help deepen the understanding of how financial entities and FMIs are operationally and technologically interconnected, the steps they have taken to guarantee the security of the information, and which transmission channels could trigger financial instability via cyber-attacks. Based on this analysis, they should develop a range of cyber contagion scenarios and use these in their joint faculties to build stronger sector-wide crisis preparedness.

Mexico would benefit from improving its public and private platforms for threat intelligence and information sharing. By exchanging cyber information and intelligence within a sharing community, financial entities can improve their defensive capabilities, threat detection techniques, and mitigation strategies. Banxico should work with the financial sector to develop an industry-wide cyber information and intelligence sharing network.

Further improvements in the response and recovery capabilities are recommended. CNBV would benefit from formalizing internal and cross-border crisis management protocols for cyber incidents, whilst both Banxico and CNBV should put in practice concrete actions in connection with the *Bases of Coordination* to improve the cross-agency crisis management framework for cyber risk.[3] By improving the coordination and cooperation between the public and private stakeholders, Mexico will be better placed to manage a systemic cyber incident. Finally, Banxico and CNBV in their joint faculties should regularly conduct market-wide cyber crisis table-top based simulation exercises, including different agencies (e.g., the Ministry of Finance and Public Credit and IPAB) and financial entities/FMIs, based on a range of extreme but plausible scenarios.

The authorities need to increase awareness within the financial sector on the cyber deterrence processes around *the Bases of Coordination*. It sets out the protocols for cyber deterrence and investigation and prosecution of cybercriminals. The responsibility for investigation and prosecution lies with the General Attorney, but there are some key challenges: for example, financial entities must formally request an investigation but are reluctant to do so, as it leads to confiscation of key

[2] For the purpose of this note, banks, nonbanks, and other types of financial institutions supervised by CNBV shall be referred to as financial entities, whilst financial market infrastructures shall be referred to as FMIs. It should be noted that CNBV has a draft regulation, which is expected to be issued this year.

[3] The Bases of Coordination is a formal agreement signed by the Ministry of Finance and Public Credit (SHCP), Banxico, CNBV, CONDUSEF, CONSAR, CNSF, FGR, ABM, AMIB, AMIS, AMIG, AMAFORE, AMSOFIPO, AAGEDE, ASOFOM, the FinTech Association, AFICO and CONCAMEX to establish the basis for collaboration, in coordination with the Trade Associations and financial entities, on information security.

assets; and there is a need to build technical expertise amongst judges and investigators to analyze the crime and evidence. Banxico and CNBV could play an effective role in issuing guidance for financial entities on how to store, handle, and administer evidence to facilitate investigations and raise awareness on the important needs for developing expertise inside financial entities and to conduct effective investigations of cyber incidents.

The authorities should improve the implementation processes around *the Bases of Coordination*. It provides a good basis for coordination and collaboration between the public and private stakeholders in Mexico, although formally there is no lead agency at this moment that is responsible for its overall implementation. The Bases of Coordination needs to be translated into operational structures, policies, and procedures, with a clear leadership structure. Banxico and CNBV should set out clearly how they will work together—with each other, with the industry, with other authorities, etc.—without compromising their individual mandates. Work is being done to formalize these structures and processes, with Banxico and CNBV proposing that they take on the role of leadership between themselves. Implementing these structures and processes should be a priority as greater coordination and cooperation will enable a more integrated and holistic approach to building cyber resilience in the financial sector.

Table 1. Mexico: Recommendations on Cyber Resilience and Financial Stability		
Recommendations and Authority Responsible for Implementation	**Timing**	**Responsible Authorities**
Strategy and Governance		
Banxico and CNBV should keep developing their cyber strategies, both in their own mandates as well as in their joint functions, for the financial sector and FMIs, with a clear vision and objectives, clear articulation of roles and responsibilities in operationalizing the strategy, initiatives and tools required to operationalize the strategy, roadmap for implementation and timelines, and estimates of resources and investment required to achieve the strategy (¶31).	I	Banxico, CNBV
Banxico and CNBV in their joint faculties should clarify their different roles and responsibilities, in terms of internal coordination and external cooperation, regarding cyber risk (¶32, 33).	NT	Banxico, CNBV
Banxico and CNBV should formalize the operational structures, policies, and procedures to operationalize the Bases of Coordination and Information Security Sensitive Incident Response Group (GRI), to enable cross-agency information sharing, cooperation, and coordination, with a clear articulation of the roles and responsibilities of the different stakeholders (both public and private) in the Mexican financial sector, with clarity on the role of the lead agency or agencies (¶34).	NT	Banxico, CNBV
Banxico and CNBV should increase their capacity to fulfill their roles in strengthening the cyber resilience of the Mexican financial sector, taking into consideration a range of different approaches, such as increased resources and tools (¶35).	NT	Banxico, CNBV
Financial system and cyber mapping		
Banxico and CNBV in their joint faculties should consider developing a cyber map of the financial sector to analyze the different transmission channels, document a range of different contagion scenarios, and develop playbooks and conduct exercises, as well as consider potential stress testing scenarios, based on these scenarios (¶45).	MT	Banxico, CNBV
CNBV should maintain a specific database of third-party service providers of systemically important financial entities and FMIs and conduct analysis to identify the critical third-party service providers and determine whether there is concentration risk in the Mexican financial system (¶46).	NT	CNBV
Cybersecurity Risk Oversight (Banxico)		
Banxico should develop and issue regulatory requirements, based on the CPMI-IOSCO guidance and its cyber strategy, for the FMIs under its oversight mandate, including SPEI (¶61).	I	Banxico
Banxico should follow a more structured and comprehensive process for cyber risk oversight. This includes utilizing a portfolio of tools and techniques to assess measures used to address cyber risk against set requirements, reaching clear conclusions, and identifying specific remedial measures or thematic findings. Such assessments and findings should be taken into consideration as part of the definition of future actions. In addition, Banxico should provide appropriate cyber training to its overseers (¶61).	NT	Banxico
1/ I Immediate (within 1 year); NT Near Term (within 1-2 years); MT Medium Term (within 3–5 years).		

Table 1. Mexico: Recommendations on Cyber Resilience and Financial Stability (concluded)		
Recommendations and Authority Responsible for Implementation	**Timing**	**Responsible Authorities**
The oversight division, within the Directorate General of Payment Systems and Market Infrastructures, should be given enough independence and resources to formally conduct thorough oversight of the SPEI payment system, or fulfill that oversight function under Banxico's mandate in any other organizational arrangement (¶62).	NT	Banxico
Banxico and CNBV in their joint faculties should collaborate to effectively operationalize their respective oversight and supervisory responsibilities for DALI, CCV, and Asigna, setting clear regulatory requirements and developing an effective process for joint cyber oversight and supervision of the aforementioned FMIs (¶61).	NT	Banxico, CNBV
Cybersecurity risk supervision (CNBV)		
CNBV should issue enforceable guidance or regulation to all its supervised financial entities on cyber risk, based on international standards and best practices (¶63).	I	CNBV
CNBV should follow a more structured approach for cyber supervision. This should include more intrusive on-site cyber risk inspections and a more structured approach to offsite supervision, including use of other supervisory tools (e.g., use of independent third-party reviews) given the limitations in resources (¶64).	NT	CNBV
Monitoring, Response and Recovery		
Banxico and CNBV should consider developing a Generic Threat Landscape (GTL) Report, which sets out the specific threat landscape of the Mexican financial system, taking into consideration the geopolitical and criminal threats unique to the jurisdiction (¶75).	MT	Banxico, CNBV
Banxico should consider conducting a full scope red team test on its IT environment, to test the full range of its protection, detection, and response controls (¶76).	MT	Banxico
Banxico and CNBV, in their joint faculties, should regularly conduct market-wide cyber crisis simulation exercises, including different agencies and financial entities, based on a range of extreme but plausible scenarios (¶77).	NT	Banxico, CNBV
CNBV should develop and document crisis communication protocols, setting out the roles and responsibilities of all the relevant stakeholders during an incident, as well as the procedures to manage an incident, whether domestic or international. This should include a playbook for different cyber scenarios (¶78, 85).	NT	CNBV
Information sharing and incident reporting		
Banxico should work with the financial sector to develop and operationalize a cyber information and intelligence sharing network (¶84).	MT	Banxico
Cyber deterrence		
Banxico and CNBV in their joint faculties could play an effective role in enhancing cyber deterrence by issuing guidance for financial entities on how to store, handle and administer evidence to facilitate investigations and by raising awareness amongst the General Attorney's office on the importance of effective investigations of cyber incidents in the financial sector (¶90).	MT	Banxico, CNBV

INTRODUCTION

A. Background: Cyber Risk as a Financial Stability Concern

1. Constantly evolving cyber threats require vigilance from the financial entities, regulators, and supervisory authorities alike. Tackling cyber risk remains a global challenge, with most authorities embarking on significant work programs to strengthen resilience in this dimension. Malicious cyber actors with varying level of sophistication continue to evolve and innovate their tactics, techniques, and procedures (TTP). The recent global threat landscape has been characterized by the exploitation of a series of critical zero-day vulnerabilities (e.g., in F5 Big-IP, MS Exchange, and Pulse Secure), supply chain attacks, ransomware attacks and distributed denial-of-service attacks.[4] Additionally, non-malicious incidents like accidental data disclosures and configuration, implementation, or processing errors continue to be an important source of cyber risk.

2. The shifts in business operating practices and use of technology in response to the COVID-19 crisis are increasing the vulnerability to cyber threats. Malicious cyber actors have been exploiting the pandemic theme, for example in phishing campaigns. During the same time, the attack surface grew due to the increased use of potentially vulnerable services and personal devices.

3. The materialization of cyber risk may have ramifications for the wider financial system, both domestic and international. While not every cyber incident at a systemically important financial entity threatens the financial stability of the jurisdiction, systemic impact resulting from a cyber incident is conceivable under certain conditions.

4. Critical supply chains are increasingly a potential source of systemic cyber events. Compromising widely adopted technology solutions could be an effective manner of impacting a group of financial entities at the same time. Due to economies-of-scale and network effects, technology diversity between entities is decreasing.[5] Financial entities are adopting common software solutions, acquiring highly similar hardware components, and migrating to a select set of global cloud service providers (CSPs). Whilst FMIs are increasingly relying on critical service providers such messaging providers. A cyber incident in the supply chain could be propagated via confidence and financial contagion channels.

5. Continuous enhancement of cyber resilience is becoming the norm as cyber incidents pose a continuing and evolving threat. Strong capabilities to timely detect anomalies and compromises, as well as respond to and recover from them, are critical in the current cyber threat landscape.

[4] Zero-day vulnerabilities are weaknesses in a system not known to security researchers, developers, and operators. If cyber threat actors discover these first, exceptional opportunities to hack high-value targets may occur.

[5] For more information, see "Nuevos participantes en el sistema financiero y estabilidad financiera" https://www.banxico.org.mx/publicaciones-y-prensa/reportes-sobre-el-sistema-financiero/recuadros/%7B06842806-020F-2CAF-6361-E1002BF16028%7D.pdf

6. The Mexican authorities, under the Financial System Stability Council (CESF) have identified cyber risk as a risk with the potential to impact financial stability. A cyber incident impacting the confidentiality, integrity, or availability of a financial entity's critical activities may have the potential to destabilize the financial system.

B. Review Scope: Banks, Nonbanks, and Financial Market Infrastructures

7. This note reviews key elements of the cyber regulatory and supervisory framework for the financial sector in Mexico. This includes: (i) the role and practices of the Mexican authorities in the development of a cyber strategy for the financial sector; (ii) development and maintenance of the cyber regulatory framework; (iii) on-site and off-site supervisory processes; (iv) cyber mapping and financial stability; (v) cyber risk related information and intelligence sharing; (vi) cyber incident reporting, monitoring, response and recovery; and (vii) cyber deterrence.[6]

8. This review is limited to the framework for financial entities that fall within the mandate of Banxico and CNBV. Supervisory practices for insurance companies (under the mandate of the National Insurance and Sureties Commission (CNSF)), pension funds (under the mandate of the National Commission for Savings for Retirement (CONSAR)) and conduct matters (under the mandate of the National Commission for Financial Services Consumer Protection (CONDUSEF)) were out of scope for this review. The designation of critical national infrastructure in the financial sector, as well as additional expectations and arrangements regarding their cybersecurity posture and resilience, were also out of scope. Finally, the review does not include a full or targeted assessment of FMIs on their observance with the CPSS-IOSCO Principles for Financial Market Infrastructures (PFMIs).

9. The FSAP team collected information from several sources. These include questionnaire answers provided by Banxico and CNBV, interviews with both authorities, the study of relevant national laws and reports published by the authorities, as well as documentation of their work.

10. Conclusions and recommendations of the FSAP review are aligned with international regulatory and supervisory good practices. As there are no binding international regulatory standards on cyber risk management, the team used internationally recognized regulatory good practice as the basis of this note. The following documents were used as a benchmark in the assessment: the FSB "Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices" in 2017; the BCBS "Cyber-resilience: Range of practices" in 2018; the IMF Departmental Paper on "Cybersecurity Risk Supervision"; and the G7 "Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector". The basis of the review in the case of FMIs was the PFMIs and CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures.

[6] The term "Mexican authorities" refers to Banxico and CNBV in this TN.

STRATEGY AND GOVERNANCE

A. Cyber Strategy

11. In 2017, the Mexican government developed a national cyber strategy, driven by an Inter-Ministerial Commission for the Development of Electronic Government (CIDGE). The strategy was based on the National Development Plan (2013-18), which aimed to promote the digitalization of Mexico, through actions such as: digital government, open data, inclusion and digital skills, health and education services through ICT, and the use of ICT in financial services, among others. The five strategic objectives of the cyber strategy were: society and rights; economics and innovation; public institutions; public safety; and national security. In order to deliver the strategy, work was to be conducted across eight areas: cybersecurity culture; capacity building; coordination and collaboration; ICT research, development, and innovation; standards and technical criteria; critical infrastructures; legal framework and self-regulation; and measurement and monitoring. In 2018, the incoming government administration published its National Development Plan (2019-2024) with revisions towards the ICT approach, namely the National Digital Strategy.

12. The National Digital Strategy (2021-24) by the Office of the President of the Republic altered the approach of the national cyber strategy. It focused its priorities on larger issues, i.e., increasing access to the internet to all parts of the population, increasing digitalization and reducing poverty. Although cybersecurity was a part of the strategy, it was limited in focus and only addressed it at a high level by requiring a "culture of information security that generates certainty and trust among users of institutional and governmental technology services". Progress in operationalizing this strategy has been slow, with a limited focus on strengthening the cyber resilience of the financial sector.

13. In the absence of an effective national cyber strategy that would address the need of strengthening the cyber resilience of the financial sector, Banxico has taken significant steps to drive the agenda. In 2016, Banxico hired an international consulting firm to review its approach to cybersecurity, which concluded that although the central bank had a reasonable level of security, it was important to strengthen its approach and capabilities given its critical role to the financial sector. Between 2017-2020, Banxico focused its efforts on protecting its information and assets; building a pro-active defense and risk prevention capability; strengthening its information security governance arrangements; and improving the end-point security of the financial entities that connect into Banxico's infrastructure. In 2021, Banxico published its latest cyber strategy, citing four key areas of focus: (1) improve its internal control functions through the Continuous Reinforcement Program; 2) expand the powers of the Cybersecurity Directorate; 3) enhance the threat intelligence function and further develop its detection, analysis, containment, response and recovery capabilities in the event of cybersecurity incidents; and 4) improve its collaboration and communication with other authorities in the event of cybersecurity incidents in the financial system. Banxico has made significant progress in enhancing its maturity, improving the infrastructure, governance arrangements, and supervision of participants that connect into the central bank operated

infrastructure. However, there has been slower progress on developing the resilience of the financial system, or FMIs as a whole.

14. CNBV has made some progress on improving the cyber preparedness of the financial entities but has no formal cyber strategy for the financial entities under its supervisory mandate. CNBV has focused its efforts in four areas: 1) setting up a specific internal unit for cyber supervision; 2) issuing cyber regulation for the most relevant sectors (banks and fintech companies); 3) executing cyber assessments as part of the authorization process of new financial entities and third-party service providers of financial entities; and 4) developing the supervision process, which includes methodologies for rating and prioritizing entities' supervision and establishing supervision procedures. However, progress made in operationalizing these four areas has been limited, as will be discussed in later sections of this note.

B. Institutional Framework

15. Banxico has the mandate of promoting the sound development of the financial system and the proper functioning of the payment systems, which entitles the central bank in cybersecurity matters. Article 2 of the Banxico Law states that *"The purpose of Banco de México shall be the provision of national currency to the Mexican economy. In pursuing this purpose, its main objective shall be to procure the stability of the purchasing power of said currency. The Bank shall also have as purposes, promoting the sound development of the financial system and fostering the proper functioning of the payment systems"*. Banxico seeks to develop an adequate framework for cybersecurity as part of these responsibilities around the financial sector and payment systems, whether in its capacity as financial regulator, an operator of payment systems or an overseer of the FMIs within its scope.

16. CNBV has the mandate to supervise and regulate financial entities comprising the Mexican financial system, in order to ensure their stability and proper functioning. It also "maintains and promotes the sound and balanced development of such system as a whole, for the protection of the interests of the public". Financial entities within its scope include: credit institutions, brokerage firms, stock exchanges, investment funds, investment fund operating companies, investment fund share distribution companies, general deposit warehouses, credit unions, exchange houses, regulated multiple purpose financial companies, popular financial companies, securities depository institutions, central counterparties, securities rating institutions, financial technology institutions, credit information companies and community financial companies, amongst others. The prudential supervision of these entities encompasses operational and technology risk, including cyber risk.

17. In Mexico, there are some non-financial authorities with a role in the cybersecurity of the financial sector. They include the Mexican CERT (an entity that reports to the National Guard, which is a part of the Ministry of Security and Civilian Protection), Information Security Specialized Committee (CESI) which is comprised of a group of specialists from different federal agencies and the General Attorney Office (FGR), and the Personal Data Protection Authority.

- **CERT-Mexico** is part of the National Guard. Its mission is to provide support to entities that have critical information infrastructure in the event of cyber incidents. Support includes the identification of threats and management of computer security incidents; serving as the contact point and coordination body inside and outside the national territory; conducting digital forensic investigations; and providing the police with technical analysis to support prosecutors.
- **CESI**'s objective is to develop the information security policies applicable to national security agencies and critical infrastructures. CESI also acts as an information-sharing group when relevant cyber threats are detected.
- The **Personal Data Protection Authority** in Mexico is the National Institute of Transparency, Access to Information and Protection of Personal Data (INAI), which is an agency at the Federal level, in charge of monitoring compliance by the public and private sectors of the regulations regarding access to information and protection of personal data.

C. Governance Arrangements

Banxico

18. A key focus of Banxico's cyber strategy has been to strengthen its internal governance regarding cyber risk. Banxico has a multiplicity of roles with regards to cybersecurity of the central bank and the financial sector. Consequently, there are a number of units within the central bank that hold cyber-related responsibilities. The key responsibility for defining and operationalizing the cyber strategies for the central bank and towards the financial sector, sits in the Directorate of Cybersecurity (DCIB), which is part of Directorate General of Comptroller and Risk Management. The DCIB is comprised of three divisions: (i) Compliance, (ii) Intelligence and Response and (iii) Policy and Innovation. Such divisions have mandates that apply to internal processes within the central bank and to the financial sector. This is described in Table 2.

19. According to Banxico's Internal Regulations, there are several units responsible for verifying financial intermediaries and entities' cybersecurity compliance with the provisions of the payment systems and market infrastructures. The Directorate General of Payment Systems and Market Infrastructures (DGSPIM), and the Directorate of IT Infrastructure (DITI) are responsible for operating the central bank operated payment systems (e.g., SPEI). Supervision of the cybersecurity requirements is a shared responsibility between DITI (for telecom infrastructure), DGSPIM (for applications of the participants in the payment systems and market infrastructures), and DCIB (for organizational cybersecurity, computing infrastructure, and cyber resilience). These units exercise their supervisory powers by carrying out on-site examinations and off-site reviews of the participant banks according to the applicable legal provisions. Within the DGSPIM, there is also an oversight division that is responsible for the oversight of the FMIs that fall within the regulatory mandate of Banxico; however, the oversight function is not currently performed on the central bank operated SPEI system.[7]

[7] SPEI, SIAC, CCEN, Clearinghouses for card transactions, Clearinghouses for mobile payments, Banxico's Derivative Trade Repository, and joint oversight-supervision responsibilities for DALI, CCV, and Asigna.

Table 2. Mexico: Responsibility of Divisions in the Directorate of Cybersecurity at Banxico	
Division	**Responsibilities**
Compliance	Design, propose and coordinate activities to assess compliance with internal regulations on cyber security and cyber resilience applicable to the systems that support the Bank's operations and processes, review activities and verification of information technology controls of the entity. This subdivision represents the 2nd line of defense to manage internal cyber security risks. Supervision and participation in the sanction process related to non-compliance with the regulation on information security, cybersecurity, and cyber resilience applicable to financial intermediaries that connect to the Bank's infrastructure, including participants in Banxico's services (payment systems, monetary policy, cash function, etc.).
Intelligence and Response	Identify risk scenarios based on cyber threat intelligence and design, propose, and implement protocols for response and reaction plans to cyber incidents within Banxico and the broader financial system. Also, this subdivision coordinates cyber resilience simulation exercises including financial entities, promotes information sharing between authorities and financial entities and develops guidelines in order to strengthen cybersecurity and cyber resilience, for example in digital forensic field.
Policy and Innovation	Define, design, and propose policies, standards, guidelines, and institutional strategies, as well as the regulation for financial intermediaries or third parties that the Bank regulates in terms of cybersecurity and cyber resilience. Assessment of compliance of cybersecurity and cyber resilience requirements before an institution is authorized to participate in a payment system operated by Banxico.

20. The Directorate of IT Infrastructure (DITI) coordinates activities to assess compliance with SPEI regulations on ICT. They can supervise ICT requirements for all the systems that support the Bank's operations and processes, including the supervision of SPEI participants. DITI can also verify compliance of ICT regulation before authorizing a participant to connect to any system managed by Banxico.

21. Banxico has made significant strides in strengthening its internal cybersecurity functions. Banxico is currently reviewing its governance structures to ensure that there is a better internal coordination and collaboration, aligned with its cybersecurity strategy. In addition, Banxico is currently working on a set of changes to its by-laws to add more clarity on the roles and responsibilities of different units that are involved in cybersecurity and cyber resilience matters.

CNBV

22. In 2022, CNBV formally established the General Direction of Information Security Supervision (DG-ISS), which is responsible for the cyber supervision of the financial entities. This is a significant step and places the CNBV ahead of many international peers, where there is still no dedicated cyber supervision unit. Although cyber supervision has been ongoing for a number of years, the restructure has separated the role of DG-ISS and the General Direction of Operational and Technology Risk Supervision (DG-OTR). The DG-ISS and DG-OTR are established in the same directorate and work closely together, given the close synergies between their responsibilities and subject matter (Box 1).

Box 1. Mexico: Responsibilities of DG-ISS and DG-OTR at CNBV

DG-ISS is responsible for, among others, the following tasks:

- Supervising and assessing that all the entities regulated by CNBV implement the risk management system related to cybersecurity which includes, among others, vulnerability and penetration tests on computing's equipment, facilities, and components; communication networks; operating systems; databases, applications, and systems that support entities' operation; and to preserve information security according to regulation.
- Supervising and assessing internal controls and regulation compliance related to cybersecurity from entities regulated by CNBV; including aspects related to confidentiality, integrity, and availability of information processed, transmitted, or stored in their own technology infrastructure and that hired from third parties.
- Establishing measures and mechanisms to preserve information security in entities regulated by CNBV, as well as coordinate with the General Direction of Information Technology the measures and mechanisms to preserve information security at CNBV.
- Coordinate with other financial and law enforcement authorities, as well as entities, actions to prevent and detect irregular operations related to information security.
- Providing opinion in cybersecurity risk matters required by CNBV's supervising general directions related to authorizations (third parties are included here).

The role of DG-OTR is to:

- Supervise and assess computing equipment, facilities, and components; communication networks; operating systems; databases, applications and systems that support entities regulated by CNBV.
- Supervise and assess internal controls and compliance with regulation related to automated systems from entities regulated by CNBV.
- Supervise and assess entities' capacity to identify, measure, monitor, limit, control, inform and disclose operational and technology risk according to regulation.
- Propose measures to entities regulated by CNBV to implement preventive, control, and audit mechanisms to timely prevent and detect irregular transactions processed through computing equipment, facilities, and components; communication networks; operating systems; databases, applications and systems that support entities' operation, or failures in their operation that can put at risk entities' or clients' resources; and
- Provide opinion in operational and technology risk matters required by CNBV's supervising general directions related to authorizations (third parties are included here).

23. Although the roles and responsibilities of the cyber supervision unit are defined, CNBV would benefit from further clarifying how DG-ISS and DG-OTR should engage with other supervisory functions, given technology and cyber are horizontal risks. For example, in the case of a major cyber incident, DG-ISS would need to work closely with the supervisor of the specific bank that has suffered the incident. Clarifying the roles and responsibilities of all functions, how they should liaise with each other in supervision and during crisis, would further enhance CNBV's ability to enhance the cyber resilience of the financial sector in an integrated and holistic manner.

D. Coordination and Cooperation

24. The Bases of Coordination is a formal agreement signed by public and private stakeholders to improve coordination and cooperation within the financial sector in the field of cybersecurity. The formal agreement was signed, amongst others, by SHCP, Banxico, CNBV, CONDUSEF, CONSAR, CNSF, FGR, Association of Banks of Mexico (ABM), Mexican Association of Brokerage Institutions (AMIB), Mexican Association of Popular Financial Companies (AMSOFIPO), Confederation of Savings and Loan Cooperatives of Mexico (CONCAMEX), and FinTech Mexico Association[8].

25. The Bases of Coordination are based on five key principles:

- Adopt and maintain updated policies, methods, and controls to identify, assess, prevent, and mitigate cybersecurity risks, which are identified, evaluated, prevented, and mitigated by the highest decision-making bodies and permeate all levels of the organization.
- Establish secure mechanisms for the exchange of information between members of the financial system and the authorities on attacks that have occurred in real time and their mode of operations, response strategies, new threats, as well as the results of investigations and studies that allow entities to anticipate actions to mitigate the risks of cyber-attacks, while protecting the confidentiality of the information.
- Promote initiatives to update the regulatory and legal frameworks that support and converge the actions and efforts of the parties, considering best practices and international agreements.
- Collaborate in projects to strengthen the security controls of the different components of the infrastructure and operating platforms that support the country's financial services, promoting the use of information technologies to prevent, identify, react, communicate, typify, and make a common front in the face of present and future threats.
- Promote cybersecurity education and culture among end users and the personnel of the entities themselves that, through continuous training, will result in an active participation to mitigate the current risks of cyber-attacks.

[8] As cyber incidents can profoundly affect operational continuity in resolution, the authorities should involve IPAB more in their work on cybersecurity and the supporting efforts for contingency planning and simulations Making IPAB a signatory to the Bases of Coordination and including IPAB in the GRI should be considered.

26. The Bases of Coordination provides a very good basis for coordination and cooperation within the financial sector and involves all the relevant stakeholders. The Bases of Coordination is an excellent example of coordination and cooperation, in comparison to international peers. Bringing together all the different stakeholders (public and private) is a significant achievement and offers great potential for Mexico to tackle cyber resilience holistically. However, the agreement itself is high level and does not have specifics on formal operational structures, policies, and procedures. Banxico and CNBV staff have drafted more detailed documentation on how to operationalize the Bases of Coordination in more concrete terms, its endorsement by institutional leadership from CNBV, Banxico, and other authorities is pending. It is important for the Bases of Coordination to be fully operationalized through such operational policies and procedures, with a clear articulation of the roles and responsibilities of the different stakeholders (both public and private), as this will improve coordination and cooperation, and enable a more integrated and holistic approach to building cyber resilience in the financial sector.

27. The Bases of Coordination also established the Information Security Sensitive Incident Response Group (GRI) to coordinate measures to prevent and resolve severe crisis situations. It comprised CNBV, Banxico, CNSF, CONSAR, CONDUSEF and SHCP, whose key objective is to collaborate and coordinate in case of a major cyber incident. This entails sharing key information with each other. The policies and operational procedures for the GRI are still being formalized. Banxico and CNBV would benefit from formalizing the operational arrangements for cross-agency information sharing, as this would improve their ability to manage a crisis in a coordinated and structured manner and would facilitate the timely sharing of vital information. Overall, the Bases of Coordination has no lead agency, although informally Banxico and CNBV have taken on the role of leadership and in their draft operational protocols, they have suggested that they take on the role of presidency of the GRI. It is important that the Bases of Coordination, GRI and the overall implementation of the agreement has a clearer leadership structure to ensure that it can be effective.

E. Resources

28. As in most jurisdictions around the world, the central banks and financial regulator in Mexico require significant additional resources and tools to fulfill their respective mandates regarding cyber risk. Both authorities have training and awareness programs in place to increase the competence of their staff members. However, given the criticality of the risk area and breadth of mandates and responsibilities between the two institutions, there is a critical need for substantial additional resources, approaches, and tools for them to effectively mitigate cyber risk to acceptable risk tolerance levels.

29. The team in charge of cyber regulation and supervision of the financial sector (CNBV) is under-resourced. The limitation in staff numbers has impacted the capacity to conduct effective regulation and cyber supervision. The delay of the issuance of the enforceable guidance or regulation is due to the lack of resources. The regulation team responsible of all technological matters consists of 3 staff members. Offsite supervision has been limited across all financial entities and onsite inspections have just started in April 2022. The cyber supervision unit is also involved in

the authorization process of new financial firms and financial entities' services providers, which are resource intensive. DG-ISS is comprised of 18 staff members, placing a significant strain on the function.

30. Although Banxico has made progress in strengthening its internal cybersecurity in recent years, its wider responsibilities for the financial sector require further capacity. Banxico plays a critical role in the Mexican financial sector, with responsibilities for FMI oversight, operations of payment systems, securing its internal security, financial stability, endpoint security of participants connecting into Banxico's infrastructure and sector wide resilience. Currently, the majority of responsibilities around cybersecurity and cyber resilience of the central bank, regulation, and oversight sits with DCIB, comprised of 43 staff members, placing a significant strain on the function.

F. Recommendations

31. Banxico should enhance its current cyber strategy, whilst CNBV should develop a cyber strategy, for their respective faculties in the financial sectors. The strategies should include:

- Clear vision and objectives, that consider all financial entities and include FMIs.
- Clear articulation of roles and responsibilities in operationalizing the strategy.
- Initiatives and tools required to operationalize the strategy.
- Roadmap for implementation and timelines.
- Resources and investment required to implement the strategy.

The purpose of a cyber strategy is to specify how to identify, manage, and reduce cyber risk effectively in an integrated and comprehensive manner across the system. Authorities should establish cyber strategies tailored to the nature, size, complexity, risk profile, and culture of their financial system. Informed by the cyber threat and vulnerability landscape, an effective cyber strategy should 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.

32. Banxico should finalize its work to clarify the different roles and responsibilities of the different units within the central bank with regards to cybersecurity. It would ensure that all relevant functions can effectively discharge their different responsibilities, both internally and for the financial sector, so that Banxico is able to enhance the cyber resilience of the central bank and the financial sector in an integrated and holistic manner, consistent with its cyber strategy. Banxico is currently working on a set of changes to its by-laws to add more clarity on the roles and responsibilities of different units that are involved in cybersecurity and cyber resilience matters.

33. CNBV should clarify the cybersecurity roles and responsibilities of DG-ISS, DG-OTR, and other supervisory functions within CNBV. It would ensure that each unit is able to cooperate and coordinate its supervisory and crisis management responsibilities in an integrated and holistic manner.

34. Banxico and CNBV should formalize the operational structures, policies, and procedures to operationalize the Bases of Coordination and the GRI, with clarity on the leadership structure. Authorities should clearly articulate the roles and responsibilities of the different stakeholders (both public and private), to ensure effective coordination and cooperation in the Mexican financial sector and enable cross-agency information sharing.

35. Banxico and CNBV in their joint faculties should explore means of increasing their capacity to fulfill their roles in strengthening the cyber resilience of the Mexican financial sector. They could take into consideration a range of different approaches, such as: increasing specialized staff numbers, recruiting highly-skilled personnel for the emission and continuous updating of the regulation, upskilling generalist supervisors and overseers in cyber risk to reduce pressure on cyber risk specialists, or using different approaches and tools to obtain increased assurance of the financial sector participants (e.g., increased use of third party independent assurance reports).

FINANCIAL SYSTEM AND CYBER MAPPING

A. Cyber Map of the Financial System

36. Banxico and CNBV would benefit from considering developing a cyber map of the financial system which is currently not in place. It should be noted that cyber mapping is an emerging field, with very few jurisdictions around the world having made any progress in its development. Mapping financial and technology connections across the sector will help identify potential systemic risks from interconnectedness and concentrations. 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 liquidity shortages, write-downs, and defaults. Identification of key nodes in the financial system—for example, the payment and settlement system, financial entities that carry out key services such as clearing and the technology systems underpinning them—should be done to understand cyber risk on a system-wide basis. The mapping of the financial sector network can be used to estimate the impact of a cyber-attack on any of the nodes. Banxico carries out analysis of interconnectedness in the financial system and understanding of financial network exposures; however, expanding this discipline into the cyber domain and understanding the operational dependencies and critical nodes would assist in managing potential systemic cyber risk.

37. Banxico and CNBV have not analyzed and documented the different transmission channels that could trigger financial instability via cyber-attacks, nor the range of different contagion scenarios that could cause disruption to the financial sector. Banxico staff view that one transmission channel are potential weaknesses at participant banks that connect into the

Banxico infrastructure (e.g., SPEI system). CNBV staff considers cloud providers and financial market infrastructures to be potential transmission channels. In terms of contagion scenarios, Banxico considers disruption to the most critical services (e.g., open market operations that transmit the monetary policy or payment systems services) as realistic contagion scenarios that could propagate through the system. However, documenting in detail the different transmission channels and the different potential contagion scenarios are important tasks that remain at hand.

38. The Financial System Stability Council (CESF) determined in the last months of 2019, to carry out a stress test exercise considering a scenario with the materialization of a cyber incident. It entailed an incident that would affect relatively large entities in the financial system. The stress exercise, which would be very useful, was due to be performed with the assistance of the World Bank. However, the execution of the stress test was suspended due to the COVID-19 outbreak.

39. CNBV carries out a capital adequacy assessment exercise with information provided by financial entities to verify their capital in adverse scenarios. It encourages financial entities to incorporate different potential risks into their management decisions. This exercise includes a cybersecurity section; however, currently this exercise does not inform the pillar one capital charge determination and how it could affect the capital adequacy assessment result.

40. CNBV's cyber stress tests do not include impact calculations on capital and liquidity buffers. Bank stress tests traditionally aim at quantifying these impacts, but stresses caused by cyber incidents are difficult to model and, compounding the difficulty, data scarcity makes the outcome less reliable. Nevertheless, this is a research area worth considering and there are early examples of cyber stress tests that include capital impact calculations.[9]

41. From Banxico's perspective, cyber stress testing can assist FMIs evaluate their ability to withstand cyber incidents with potential systemic impact. A key scenario of the stress test is the disruption of payments. In the event of a cyber incident the CPMI-IOSCO expects the FMI to honor critical payment obligations by the end of the value date.

B. Outsourcing and Third-Party Risk

42. Banxico and CNBV have strong controls to ensure that financial entities manage their outsourcing and third-party risk. Although there is no specific regulation that enables Banxico to have direct access to third-party service providers of their supervised entities, the central bank can oblige financial entities to set out specific requirements in their contracts with such critical third parties. CNBV, on the other hand, has a suite of regulations (e.g., Law of Credit Institutions, Popular Savings and Credit Law, Law of Financial Cooperatives and FinTech Law) that empowers CNBV to manage risks stemming from third-party service providers. The regulations require:

[9] See Bouveret (2018), https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924.

- Financial entities to ensure that there are contractual clauses that allow CNBV to carry out inspections of third-party service providers, or financial entities themselves to carry out audits of the third parties.
- Financial entities to report to CNBV, in advance, any change in the core activity of the service provider to allow an evaluation and subsequent approval.
- Financial entities to ensure that third-party service providers are subject to strict confidentiality terms regarding the operations of the financial entity and clients' information.
- Financial entities to evaluate the criticality of the outsourced service and estimate the impact that it would have on their operations if that provider would no longer be available.
- Financial entities to establish policies for the proper management, control and security of information related to third-party services.
- The contracts to stipulate restrictions and conditions of sub-contracting by the third party.
- CNBV to approve the outsourcing to third-party service providers.

43. In the case of banks and financial technology firms, the regulations apply to the use of foreign-based cloud computing services. Given the complex challenges of cloud computing and the transmission of data, the regulations ensure that banks must notify CNBV in advance (for approval) if they seek to outsource to a cloud provider in a foreign jurisdiction. In these cases, the cloud provider must be based in countries whose internal law provides client's data protection, safeguarding their confidentiality, or there must be an international agreement with Mexico in such matters, and their financial supervisory bodies must have collaboration agreements with the Mexican financial authorities for the exchange of information. Additionally, if contracting to foreign providers, the banks must assure CNBV that by contracting such services: (i) their regulatory compliance is not at risk, (ii) the business practices of the third-party service provider are consistent with those of the entity itself, and (iii) there would be no impact on the financial stability or operational continuity of the entity, due to the geographical distance or language.

44. Despite having a robust regulatory framework and approval process for third-party service providers, CNBV does not maintain a specific database of critical third-party service providers of systemically important financial entities. At the time of this review, although CNBV collects the information related to all third-party service providers, it does not have a specific list or database to quantify the percentage or number of its supervised financial entities that have migrated to the cloud. In recent years outsourcing and third-party risk has been on both the macroprudential and micro-prudential supervisory agenda, especially given the significant cyber risk stemming from the supply chain. Large and concentrated third-party service providers are increasingly a transmission channel for financial instability, especially if they are subject to a major cyber incident that can cause operational disruption or data loss across its large customer base of financial entities that rely on them. CNBV would benefit from aggregating the list of third-party

services providers, including cloud providers, that the Mexican financial system depends on. The list of providers would benefit from being integrated into the cyber map and would allow CNBV (and Banxico) to better identify the critical nodes in the system, determine whether there is any concentration risk, build contagion scenarios stemming from such providers and therefore also help inform any policy decisions that may be required to reduce systemic risks.

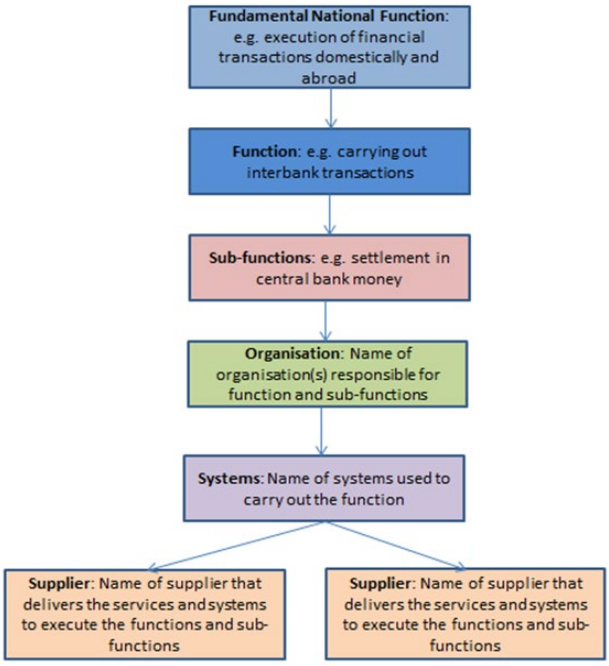
C. Recommendations

45. Banxico and CNBV should, for their joint faculties:

- Develop a cyber map of the financial sector, which includes identification of critical service providers to FMIs and financial entities.
- analyze the different transmission channels and document a range of different contagion scenarios.
- analyze the steps that financial institutions have taken to secure the information transmitted and to establish accountability rules for all point-to-point connections between all systems.
- develop playbooks and conduct exercises, as well as consider potential stress testing scenarios, based on these scenarios.

In developing the cyber map, Banxico and CNBV could consider the approach in Figure 1.

Figure 1. Mexico: Structure of Possible Financial Sector Cyber Map



Source: IMF Staff.

46. CNBV should maintain a specific database of third-party service providers of systemically important financial entities. It should conduct analysis to identify the critical third-party service providers and determine whether there is concentration risk in the Mexican financial system.

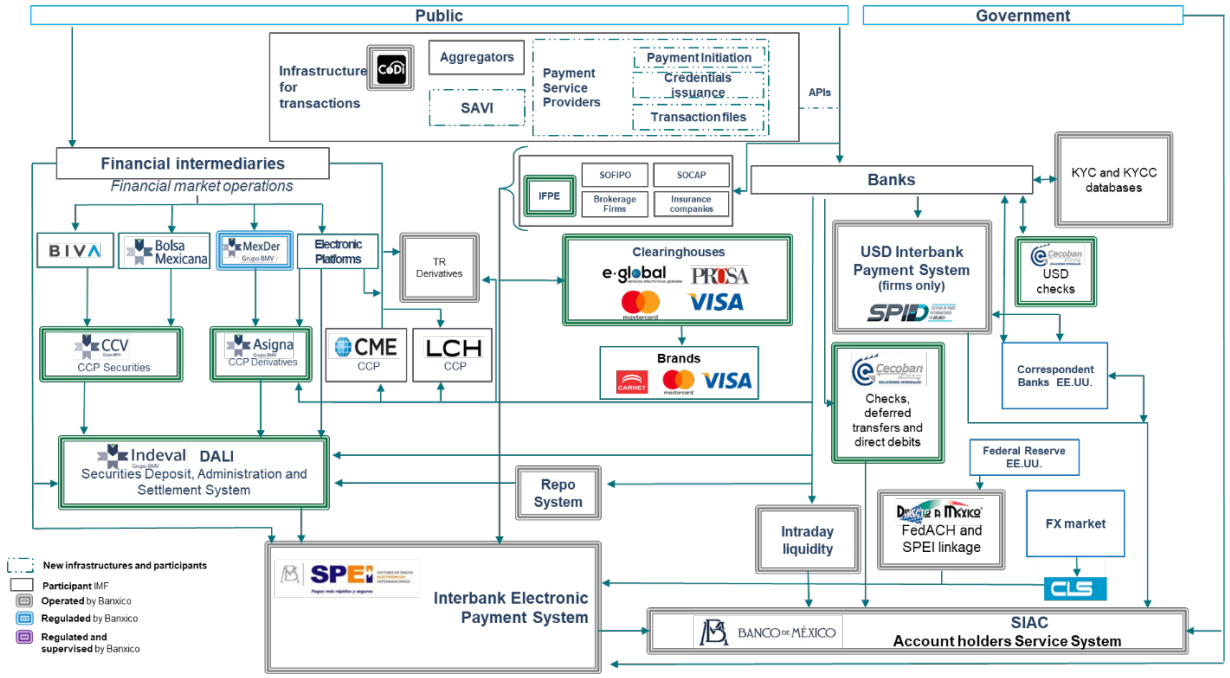
CYBER REGULATORY FRAMEWORK AND SUPERVISORY PRACTICES

A. FMI Cyber Oversight

47. Mexico has a complex FMI landscape, in which Banxico plays a pivotal role as regulator, overseer, operator, and user (Figure 2). All the national FMIs are regulated by Banxico. In some cases, the regulatory role lies entirely with Banxico, whereas in others, the central bank shares its responsibilities as a regulator with CNBV. As a regulator, the central bank both proposes and issues regulation. Banxico takes measures to monitor compliance with regulation related to FMIs, both by operators and participating financial entities. Banxico is the administrator and operator of SPEI and SIAC. The central bank provides electronic funds transfer services through SPEI. Additionally, it provides liquidity to banks and access to central bank accounts for financial entities and some public entities through SIAC. Furthermore, Banxico and the U.S. Federal Reserve jointly manage and operate the system that allows users to send money to Mexico, namely, *Directo a México*. Lastly, Banxico operates a Derivatives Trade Repository. The central bank implements monetary policy through the national FMIs. The results of the open market operations through which liquidity is provided are formalized as collateralized loans; the resources are credited to banks through SIAC, or alternatively, repos are settled in DALI. Liquidity withdrawal operations are formalized as deposits with resources from banks' SIAC accounts. Banxico, in its role as the financial agent of the federal government, manages and places federal government bonds in domestic currency. Additionally, it acts as a placement agent for the Institute for the Protection of Bank Savings (IPAB). To conduct these activities, Banxico uses the DALI system.

48. Given the systemic role of FMIs in Mexico, effective regulation and oversight is critical from a financial stability perspective. There are four statutes authorizing Banxico to oversee FMIs: (i) the Banxico Law establishes as one of the central bank's purposes the aim of fostering the proper functioning of the payment systems, and it empowers the bank to supervise intermediaries and financial entities based on regulations the central bank issues; (ii) the Payment Systems Law authorizes the central bank to monitor the supervisory systems subject to this law; (iii) the Securities Market Law empowers the central bank to request information and authorize changes to the internal regulations of securities central counterparties and securities settlement systems within the scope of its powers; and (iv) the Transparency and Regulation of Financial Services Law empowers the central bank to supervise clearinghouses.

Figure 2. Mexico: FMI Landscape



Source: Banxico's Financial Market Infrastructures Annual Report, 2020 (Original in Spanish).

49. Banxico has formal oversight responsibilities for the following FMIs: SPEI, SIAC, CCEN, Clearinghouses for card transactions, Clearinghouses for mobile payments, Banxico's Derivative Trade Repository, and joint oversight-supervision responsibilities for DALI, CCV and Asigna with CNBV. The oversight of FMIs is carried out by the oversight division within DGSPIM. The division is staffed with FMI overseers, who are responsible for oversight of all the FMIs in scope, but without dedicated cyber specialists. To fill this void, the department works closely with DCIB, which provides technical expertise and insight.

50. The cyber oversight approach of Banxico could be further substantially strengthened, as set out below:

- There is no formal oversight of the Banxico operated systems (e.g., SPEI), although the systems are subject to the internal rules regarding non-financial risks, business continuity and cybersecurity for Payment Systems operated by Banxico.
- The FMIs under the mandate of Banxico are not subject to specific, harmonized, and enforceable cyber guidelines or expectations—including DALI, CCV, and Asigna, which are jointly regulated and supervised by Banxico and CNBV.
- The FMIs have not been assessed for their cybersecurity neither through offsite nor onsite oversight.

- There is no structured process and methodology for cyber onsite and offsite oversight of the FMIs.

- Banxico and CNBV have not conducted any joint cyber oversight of DALI, CCV, and Asigna.

51. Despite the lack of formal oversight of the Banxico operated systems (e.g., SPEI), it should be noted that Banxico applies the three lines of defense. The three lines of defense model used by Banxico includes operations, risk management, internal control/compliance and internal audit to operate the SPEI system. It benefits from strong cybersecurity and operations units that is well supported by risk management, internal control and internal audit. Within this context, the Banxico systems, including SPEI, are subject to comply with security requirements set by DCIB, unlike some other external, private FMIs that fall within the oversight mandate of Banxico. This creates an uneven level playing field. The security requirements are based on NIST 800-53 and ISO 27000. The DCIB issues cybersecurity requirements for the SPEI system operation, sets the controls for the Banxico systems and thereafter, now as second line of defense, reviews the first line's compliance against them. The second line validates 136 security controls, which encompass people, processes, and technology, and assesses the effectiveness of these controls on a 3-year workplan, ensuring all controls are reviewed within this timespan. Additionally, the internal audit function will review the Banxico systems every two years as part of their audit plan. However, despite an effective three lines of defense model, there is an important need for the formal oversight of the Banxico systems, such as SPEI, as it is understood under the CPMI-IOSCO Principles, to ensure a level playing field with other Mexican FMIs.[10] Banxico should adopt the CPSS-IOSCO PFMIs and ensure that these principles are, at a minimum, applied consistently to all systemically important payment systems, CSDs, SSS, CCPs, and TRs. This should seek to improve the observance of Responsibility A and D of the PFMI."

52. The safe and efficient operation of FMIs is essential to maintaining and promoting financial stability and economic growth. If not properly managed, FMIs can be sources of financial shocks, such as liquidity dislocations and credit losses, or a major channel through which these shocks are transmitted across domestic and international financial markets. In this context, the level of cyber resilience, which contributes to an FMI's operational resilience, can be a decisive factor in the overall resilience of the financial system and the broader economy. It is therefore critical that there is a robust regulatory framework and an effective, continuous, and structured oversight approach for FMIs. The lack thereof poses a significant risk to financial stability.

53. Despite the gaps in cyber oversight of the FMIs, Banxico conducts rigorous and effective supervision of participants, to ensure that they connect into Banxico's infrastructure with adequate cybersecurity. Banxico has set security requirements for participant banks that connect into the Banxico infrastructure, based on NIST 800-53 and ISO 27000. The off-site supervision process consists of reviewing cybersecurity controls in telecommunications and

[10] Under Responsibility A of the CPSS-IOSCO Principles for Financial Market Infrastructures (PFMIs), FMIs should be subject to appropriate and effective regulation, supervision, and oversight by a central bank, market regulator, or other relevant authority, including the central-bank operated SPEI system.

computer infrastructure and systems applications. The supervision staff performs off-site reviews using information that financial entities provide to Banxico regarding their compliance with the cybersecurity requirements. The information requested has yes or no questions and financial entities must provide evidence to support their answers.

54. The supervision staff perform on-site examinations by visiting the facilities and offices of financial entities, with the purpose of verifying their compliance with the cybersecurity requirements established in the applicable system rules. Banxico authorizes its inspectors to carry out interviews and gather evidence to support the findings. The supervisor communicates all the findings to the entity. The entity elaborates a working plan to solve any issues identified in the examinations. The controls evaluated reviewed in offsite and onsite reviews cover:

- Cybersecurity organizational structure.
- Access control.
- Internet access.
- Network segmentation.
- Network access.
- Antivirus and malware protection.
- Vulnerability assessment and management.
- Penetration test assessment for third parties.
- Software and services management.
- Cyber incident response and report.
- Encryption of sensitive information.
- Integrity and non-repudiation mechanisms.
- Encrypted communications.
- File Integrity monitoring; and
- Audit logs.

55. Since 2018, Banxico has conducted 126 reviews of financial entities' cybersecurity compliance with the system rules. The review of financial entities' controls against the requirements of the Banxico infrastructure is a core part of the *"CPMI Strategy for Reducing the risk of wholesale payments fraud related to endpoint security,"* which Banxico is leading effectively and

comparatively better than other jurisdictions.[11] However, the results of reviews conducted by Banxico are not shared with CNBV, the prudential supervisors of these financial entities. A core part of the CPMI strategy is to improve the coordination and information sharing between banking supervisors, operators of the SPEI system and the FMI overseers. Sharing the cybersecurity weaknesses of participant banks with CNBV (if legally feasible), would provide CNBV with invaluable information about the potential cybersecurity strengths and weaknesses of their supervised entities and would facilitate risk-based intervention by the supervisor (if needed).

B. Cyber Supervision

56. Currently, CNBV has regulation on cybersecurity only for banks, brokerage houses, and financial technology institutions. Given the broad range of financial entities within the scope of CNBV's supervision, there are significant entities in Mexico that are not currently subject to enforceable cyber regulation or guidelines. This poses a risk to the financial system as a whole, given the interconnectedness of the financial system; weaknesses in some entities could propagate through the whole system. It is therefore essential that Mexican financial entities under the scope of CNBV are subject to detailed and comprehensive cyber regulation, including DALI, CCV, and Asigna, which are jointly regulated by Banxico and CNBV.

57. The current regulation applicable to banks spans approximately 600 pages and encompasses requirements for banks across all risk categories. Consequently, the requirements related to cybersecurity, operational, and technology risk are scattered throughout the regulation making it difficult for banks to access and discern a clear suite of requirements. The requirements are focused on:

- implementing an Internal Control System for Information Security.
- designing, implementing, and maintaining a strategy.
- designing and executing penetration tests and vulnerability scanning, and their respective remediation plans.
- designing, implementing, and monitoring information security training programs.
- roles and responsibilities of a Chief Information Security Officer (CISO).
- roles and responsibilities of the CEO.
- operation and security configurations of each component of the infrastructure, from acquisition or development to implementation, changes and, where appropriate, replacement.

[11] The strategy is designed to be taken into account by all relevant public and private sector stakeholders in reducing the risk of wholesale payments fraud, including operators of wholesale payment systems and messaging networks, their participants and the respective regulators, supervisors and overseers of these operators and participants. See: https://www.bis.org/cpmi/publ/d178.pdf

- security measures for components of the infrastructure.
- security measures for the information that is transmitted, stored, and processed, such as: identification and authentication mechanisms, encryption processes, access keys, controls for physical access, environmental and electrical energy controls.
- assessing information security risk level through key risk indicators.
- security measures for transactions' end points.
- backups and recovery of information.
- audit trails.
- information security incident management processes.
- setting up an incident response team.
- mechanisms to prevent the loss, alteration, and extraction of information.
- processes to measure and ensure availability levels and response times.
- manual and automated mechanisms to detect and prevent information security events and incidents.

58. Although the current regulation for banks includes some key cybersecurity requirements, the regulation could be better structured in line with international standards and best practices. The regulation could follow a more logical and systematic sequence of requirements, as laid out in standards such as NIST 800-53 and ISO 27000. It should be noted that CNBV is currently undertaking a regulatory initiative to update and standardize the existing cyber regulation and to extend it to other sectors. It is developing a single, unified regulatory document containing all relevant cybersecurity aspects applicable to financial entities. Although the timelines for this initiative are unclear, this would be an important step to ensure consistency and a level playing field for all supervised entities. It is important that CNBV uses international standards as an inspiration in developing a unified cyber regulation, which covers the following essential categories: governance; risk assessment and identification; protection; detection; response and recovery; testing; outsourcing; and situational awareness.

59. The cyber supervision approach of CNBV requires significant improvements, as set out below:

- CNBV has only started to conduct cyber onsite inspections of its supervised entities in April 2022, largely due to limitations in its resources; however, CNBV has developed effective supervisory manuals and processes, and a robust methodology to evaluate and prioritize the

cyber risk of financial entities, called "Rating of Financial Entities with an Information Security Risk Approach" (CEFER-SI), which provide a good basis for future cyber supervision.

- CNBV relies heavily on its offsite supervision, however, the processes and tools to administer offsite supervision is limited. CNBV focuses its offsite supervision on governance, the organizational structure of the entity's Information Security area, its functions, job descriptions and reports to audit and risk committees; results from vulnerability and penetration tests, which includes remediation actions; incident reports; and key risk indicators. However, as yet, financial entities (e.g., banks) which are subject to cyber regulatory requirements have not provided CNBV with any self-assessment against the regulations. The overall regulatory information provided by entities is limited in scope and does not allow CNBV to comprehensively monitor the cybersecurity posture of the entities.

- CNBV does not use third-party independent reviews as part of its supervisory toolkit to gain assurance on the financial entities it supervises. The use of such reviews can increase the level of assurance for the supervisors and maximize efficiency in supervision, given CNBV's resource constraints. In some jurisdictions (e.g., U.K. Banking Act 2009 and ECB SIPS Regulation), supervisors will hold the powers to mandate an independent review of an entity on a key risk area, at the expense of the entity, to further supplement the authority's supervision.

- Banxico and CNBV have not conducted any joint cyber supervision of DALI, CCV, and Asigna.

60. Given the interconnectedness of the financial entities under the mandate of CNBV, it is essential that CNBV establishes a comprehensive cyber regulatory framework and operationalizes a cyber supervisory framework. The framework should combine effective offsite, on-site, and thematic supervision, using a diverse range of tools. Regulation and supervision set consistent minimum standards to be used by financial entities, including promoting good cyber hygiene and setting expectations for risk management practices, incident reporting, and response and recovery protocols, as well as internal governance procedures. Effective cyber regulation and supervision would allow CNBV identify entities with weak cybersecurity and take appropriate remedial action, leading to a more resilient financial system.

C. Recommendations

61. The cyber risk oversight of FMIs should be significantly enhanced. Banxico should:

- Provide cyber training to its FMI overseers, and as needed, leverage the capacity with the expertise on cybersecurity in the DCIB and the authorities' cyber strategy;

- Set clear regulatory requirements for all the FMIs under its mandate, leveraging the CPMI-IOSCO cyber guidance and on the new enhanced cyber strategy. By setting clear requirements, Banxico will: (i) provide its overseen FMIs with detailed steps on how to operationalize the CPMI-IOSCO guidance, ensuring they are able to foster improvements and enhance their cyber resilience over a sustained period of time; (ii) establish a clear basis against which it can assess the FMIs it is

responsible for; and (iii) provide the basis for a meaningful discussion between the FMIs and the overseers. When establishing these expectations, Banxico should ensure that these are communicated clearly to the FMIs;[12]

- Develop and operationalize a more structured and comprehensive cyber oversight approach. This includes utilizing a diverse portfolio of tools and techniques to assess against the set requirements, culminating in clear conclusions and identifying specific remedial measures and/or thematic findings that can lead to future action. A more structured and intrusive approach would allow Banxico to gain greater assurance on the FMIs and their critical service providers. This should be supported by an adequate number of staff and a toolkit for cybersecurity assessment, which may include, but are not limited to, questionnaires, self-assessments, desktop reviews of documentation, on-site inspections and walkthroughs, and technical reviews ("deep dives") on key risk areas. The toolkit and assessment process will allow Banxico to develop clear conclusions and identify concrete remedial measures that can lead to future action; and

- Collaborate with CNBV to effectively operationalize its oversight responsibilities for DALI, CCV, and Asigna, setting clear regulatory requirements and developing an effective process for overseeing and supervising the aforementioned FMIs.

62. The payment system oversight division within DGSPIM should be given adequate independence[13] and resources to conduct thorough oversight of the Banxico operated systems (e.g., SPEI), or it should be conducted in any other organizational arrangement that Banxico defines.

63. CNBV should issue enforceable guidance or regulation to all of its supervised entities on cyber risk, based on international standards and best practices.

64. CNBV should follow a more structured approach for cyber supervision. This should include more intrusive on-site cyber risk inspections and a more structured approach to offsite supervision. This includes utilizing a diverse portfolio of tools and techniques to assess against the set regulation, culminating in clear conclusions and identifying specific remedial measures and/or thematic findings that can lead to future action. A more structured and intrusive approach would allow CNBV to gain greater assurance on their supervised entities. This should be supported by an adequate number of staff and a toolkit for cybersecurity assessment, which may include, but are not limited to, questionnaires, self-assessments against the regulation, desktop reviews of

[12] Banxico should take note of and address issues of concern, if any, that are relevant for Mexican FMIs as reported to the CPMI-IOSCO Level 3 assessment of FMI cyber resilience as part of the oversight approach. This includes issues relating to the development of cyber response and recovery plans to meet the two-hour recovery time objective, cyber resilience testing, comprehensive scenario-based testing, and inclusion of FMI participants, critical service providers and linked FMIs in the testing of response, resumption, and recovery plans.

[13] In line with international best practices, the independence should ensure that there is clear separation between the overseer of the SPEI and the operator of SPEI, to avoid any potential conflict of interest and to establish a level playing field in the manner Banxico conducts its oversight of all FMIs – both private and central bank operated. A central bank should be careful to protect confidential information collected in its role as overseer and avoid its misuse.

documentation, on-site inspections and walkthroughs, and technical reviews ("deep dives") on key risk areas. Given the limitations in resources, CNBV should consider using other means of maximizing assurance on its supervised entities, such as use of independent third-party reviews (conducted by auditors) as a supervisory tool.

MONITORING, RESPONSE, AND RECOVERY

A. Monitoring

65. Banxico monitors the threat landscape by using a variety of different sources, based on collaboration with public, private, domestic, and international agencies. Banxico gathers cyber threat intelligence from three types of sources:[14] (i) open sources like the internet, social media, deep web and dark web; (ii) sources like Group-IB (their current commercial threat intelligence provider), the Financial Services Information Sharing and Analysis Center (FS-ISAC) and SWIFT ISAC;[15,16] and (iii) other authorities, both domestic (e.g., CERT-Mexico) and international (e.g., OSSAT which is a network of international central banks).[17]

66. CNBV monitors the threat landscape by gathering cyber threat intelligence from three types of sources: (i) open sources like Internet, social media, deep web and dark web; (ii) commercial sources like Minsait (their current commercial threat intelligence provider), and (iii) other Mexican financial authorities, such as CERT-Mexico. Additionally, CNBV receives information of security events and incidents from reports of supervised entities.

67. Banxico and CNBV confirmed that the evolution of cyber threats in Mexico during the COVID-19 crisis is the same as in other jurisdictions. They include DDoS attacks, ransomware, advanced persistent threats (APTs) in the electronic funds transfer applications, and ATM malware injection combined with physical damage to the devices. In this context, it is important to note that during the pandemic, ransomware constituted one of the major concerns for financial entities in Mexico.

68. Based on its incident reporting regime, CNBV and Banxico gather incident information from its supervised entities and publish an annual report of the relevant incidents on Banxico´s website. The incidents from 2020-21 are cited in Table 3.

[14] Cyber threat intelligence (CTI) is knowledge, skills and experience-based information concerning the occurrence and assessment of both cyber and physical threats and threat actors that is intended to help mitigate potential attacks and harmful events occurring in cyberspace. Cyber threat intelligence sources include open-source intelligence, social media intelligence, human intelligence, technical intelligence, device log files, forensically acquired data or intelligence from the internet traffic and data derived from the deep and dark web.

[15] Financial Services Information Sharing and Analysis Center.

[16] SWIFT Information Sharing and Analysis Center.

[17] European Central Bank's Operational Security Situational Awareness Secretariat.

69. Banxico and CNBV have a broad range of sources to collect cyber threat intelligence, and in conjunction with information from incidents in the sector, provide a good basis for the authorities to understand the threat landscape for Mexican financial system. However, both authorities could improve their overall analysis of the threat landscape by combining the different sources and developing a Generic Threat Landscape (GTL) Report. The GTL Report could elaborate on the specific threat landscape of the Mexican financial system, taking into consideration the geopolitical and criminal threats unique to the jurisdiction. The report could consider key financial market participants and their critical functions, including (wholesale and retail) banks, broker-dealers, financial market infrastructures, financial market utilities, 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 entities to better prepare for potential attacks through scenario development, building playbooks and exercising.

70. Banxico monitors its cybersecurity capabilities by conducting red team tests on its IT environment, however, the scope of such tests has been limited to specific applications and systems. Red team tests mimic the tactics, techniques, and procedures (TTPs) of real-life threat actors who, on the basis of threat intelligence, are perceived as posing a genuine threat to entities. A red team test involves the use of a variety of techniques to simulate an attack on an entity's critical functions (CFs) and underlying systems (i.e., its people, processes, and technologies). It helps an entity to assess its protection, detection, and response capabilities. Banxico has conducted red team tests, but these tests have been limited to specific applications and systems. Banxico could benefit from a full-scope red team test on the central bank's infrastructure, to test the full range of its protection, detection, and response controls. This would allow Banxico to monitor its security based on a sophisticated test and find any weaknesses and vulnerabilities that need remediation.

Table 3. Mexico: Cyber Incidents During 2020–2021

Year	Type of cyber attack	Targets	Estimated losses in millions of Mexican Pesos	Brief description
2020	Ransomware	Internet banking	Pending	Servers of a commercial bank were infected with ransomware.
	Ransomware	Bank tellers	Pending	Computers of a commercial bank branch were infected with ransomware.
	Ransomware	Dispersal of funds	Pending	Servers of a brokerage firm were infected with ransomware.
	Ransomware	Internet banking, foreign exchange operations, dispersal of funds	Pending	Servers of a financial group were infected with ransomware.

Table 3. Mexico: Cyber Incidents During 2020–2021 (concluded)				
Year	**Type of cyber attack**	**Targets**	**Estimated losses in millions of Mexican Pesos**	**Brief description**
2021	Infrastructure	ATM	0.63	ATMs of a credit institution were attacked.
	Infrastructure	ATM	0.13	ATMs of a credit institution were attacked.
	Ransomware	Internet banking	Pending	Servers and terminals of a credit institution were infected with ransomware (REvil, also known as Sodinokibi).
	Infrastructure	ATM	8.10	ATMs of a credit institution were attacked.
	Infrastructure	ATM	0.80	ATMs of a credit institution were attacked.
	Infrastructure	ATM	3.01	ATMs of a credit institution were attacked.
	Infrastructure	Transfers on branches	474.40	The transfer of funds on branches system of a credit institutions and its brokerage firm.
	Infrastructure	ATM	4	ATMs of a credit institution were attacked.
	Infrastructure	ATM	0. 73	ATMs of a credit institution were attacked.
	Applications	ATM	79	The funds transfer application of a credit institution was attacked to withdraw cash from ATMs without the need of a card.

B. Response and Recovery

71. Banxico has conducted two cyber crisis simulation exercises. During 2021, Banxico coordinated two table-top cyber resilience exercises and included the five systemically important banks. Banxico hired two consultants to assist them in coordinating the exercises, as well as participating in them. The table-top scenarios considered a ransomware attack, APT attack, and data breach in the IT infrastructure of Banxico that provides: (i) international funds transfers to administer the international Reserves(ii) auctions for monetary policy implementation; and (iii) the web-based regulatory information reporting system. The goal was to test and improve incident response, communication, crisis management, and recovery capabilities of all participants against cyber-attacks. The exercises were well structured, with good scenarios and act as a good basis for further similar exercises.

72. CNBV have not been involved in industry-wide cyber crisis simulation exercises and does not coordinate any exercises with its supervised entities. However, in March 2021 CNBV participated in an exercise carried out by other agencies of the Federal Government and the CERT-Mexico, but financial entities did not participate. In this exercise CNBV carried out the exchange of public keys for the secure distribution of information, and an attack simulation was carried out where each participant assessed the impact of the attack, shared relevant information with the rest of the participants, and proposed preventive and corrective activities. Additionally, as part of the international collaboration initiatives in the Pacific Alliance, CNBV is intending to carry out a cyber crisis simulation exercise with some financial entities.

73. The goal of the industry-wide cyber crisis simulation exercise is to rehearse the collective response of the financial sector to major operational disruption. The attack scenarios can vary, but the focus is on collective response capacity. These exercises aim to: (i) test the

effectiveness of decision-making and crisis communication arrangements; (ii) validate collective contingencies; (ii) enable participants to practice their response protocols; and (iv) to improve the sector-level response coordination between the public and private, and with other jurisdictions. Such exercises can identify gaps in operational resilience of entities and of financial systems, helping to identify priorities that strengthen response and recovery capabilities. Exercises can also point to gaps in information sharing arrangements and support collective action to address them. Banxico and CNBV should conduct regular exercises with each other, other authorities, and a broader selection of financial entities (e.g., banks, FMIs, insurance companies, third-party providers, etc.).

74. CNBV has not documented any crisis communication protocols if there is a large-scale cyber-attack, nor any playbook for different cyber scenarios. Banxico has crisis communication protocols and based on the two cyber crisis management exercises conducted, Banxico has developed playbooks for different cyber scenarios, i.e., ransomware, advanced persistent threats, web attacks, data breaches, and denial of services. Conducting regular exercises will allow CNBV and Banxico to develop (or further enhance) crisis communication protocols and playbooks for different scenarios, and then test their effectiveness.

C. Recommendations

75. Banxico and CNBV should consider developing a Generic Threat Landscape (GTL) Report. The report could set out the specific threat landscape of the Mexican financial system, taking into consideration the geopolitical and criminal threats unique to the jurisdiction. The report could also consider key financial entities and their critical functions, the different threat actors (including their tactics, techniques, and procedures) targeting these entities, and the common vulnerabilities.

76. Banxico should consider conducting a full scope red team test on its ICT environment. The red ream needs to test the full range of its protection, detection, and response controls. This would allow Banxico to monitor its security based on a sophisticated test and find any weaknesses and vulnerabilities that need remediation.

77. Banxico and CNBV should regularly conduct market-wide cyber crisis simulation exercises. The exercise should include different authorities and financial entities and be based on a range of extreme but plausible scenarios, to improve the financial sector's ability to response and recover effectively to a cyber incident.[18] The goal of industry-wide cyber crisis management exercises is to rehearse the collective response of the financial sector to major operational disruption.

78. CNBV should develop and document crisis communication protocols if there is a large-scale cyber-attack, as well as playbooks for different cyber scenarios.

[18] From an FMI perspective, such exercises allow authorities to assess FMI capabilities in meeting the two-hour recovery time objective and end of day settlements following a market-wide cyber crisis simulation.

INFORMATION SHARING AND INCIDENT REPORTING

A. Information Sharing

79. Although Banxico is part of a number of international information sharing groups, i.e., FS-ISAC, SWIFT ISAC and OSSAT, there is no effective industry-wide information and intelligence sharing network in the Mexican financial sector.[19] Notwithstanding the lack of an industry-wide information and intelligence sharing network, the Bases of Coordination sets out the requirement for public and private sectors to collaborate to strengthen the cybersecurity of the financial system in Mexico, including information sharing.[20]

80. Although the requirement for information sharing has not been fully operationalized, there have been some positive steps. There is a consortium of seven large banks, from the ABM, that have established an information sharing network amongst themselves. Banxico is in the process of setting a MISP instance to connect into the information sharing network run by the ABM.[21] However, there are challenges in the current set-up: the network of the consortium of seven banks excludes most financial entities in Mexico and the market has stressed their reluctance to share information in a network that may include regulators and supervisors.

81. Amongst other things, financial entities should have effective cyber threat intelligence processes and actively participate in information and intelligence sharing arrangements and collaborate with trusted stakeholders within the industry. Cyber threat intelligence is any information that can help a financial entity identify, assess, monitor, defend against and respond to cyber threats. By exchanging cyber intelligence within a sharing community, financial entities can leverage the collective knowledge, experience, and capabilities of that sharing community to gain a more complete understanding of the threats they may face. Using this knowledge, members of the community can make threat-informed decisions regarding defensive capabilities, threat detection techniques and mitigation strategies. The Mexican financial sector would benefit greatly if Banxico engages with the financial sector to develop an industry-wide information and intelligence sharing network.

B. Incident Reporting

82. Banxico and CNBV have comprehensive cyber incident reporting regimes in place. Their approach places them ahead of other jurisdictions, where developing and operationalizing an

[19] It should be noted that such industry-wide sharing networks are limited in other jurisdictions and significant global progress is required in this area. Some examples of such networks are CIISI-EU in the EU and the Cyber Defense Alliance in the United Kingdom.

[20] "Establish secure mechanisms for the exchange of information between the members of the financial system and the authorities, on attacks that have occurred in real time and their mode of operation, response strategies, new threats, as well as the results of research and studies, which allow the entities anticipate actions to mitigate the risks of cyber-attacks, while protecting the confidentiality of information."

[21] MISP (formerly known as Malware Information Sharing Platform) is an open-source threat intelligence and sharing platform. It is a platform for sharing, storing and correlating Indicators of Compromises of targeted attacks but also threat intelligence such as threat actor information, financial fraud information and many more. A MISP instance is a mini-platform, set up at an entity, that can be connected to a centralized MISP platform or other similar instances at entities on a decentralized basis. MISP is managed by the Computer Incident Response Centre in Luxembourg (CIRCL).

incident reporting regime remains a key challenge. Financial entities must report cyber incidents to their respective financial authorities. The approach for incident reporting of Banxico and CNBV is set out in Table 4.

83. Whilst Banxico has a documented incident response framework and crisis communication protocols, CNBV does not. CNBV is the supervisor of domestic and international financial entities. The international dimension of financial entities adds a level of complexity to incident management. Currently, CNBV has informal processes to manage an incident, with the cyber supervision unit taking the lead. Informally, the cyber supervision unit will liaise internally with the relevant financial supervisor and/or the international supervisor if the incident relates to a foreign bank or inform the GRI (if relevant). However, the crisis communication protocols are not documented and CNBV would benefit from documenting the roles and responsibilities of all the relevant stakeholders during an incident, as well as the procedures to manage an incident, whether domestic or international. This documentation would allow CNBV to effectively manage a range of different plausible scenarios, improve the preparedness of the institution and its personnel to manage a crisis that could become systemic, and enhance cross-agency and cross-border coordination.

Table 4. Mexico: Cyber Incidents Reporting Regimes

	Banxico	CNBV
Is there a cyber incident reporting regime in place?	Yes	Yes
Does the authority routinely collect data on cyber incidents?	Yes	Yes
What incidents must be reported?	Banxico uses the definition of an incident cited in the Bases of Coordination: "An assessed event that actually or potentially jeopardizes the confidentiality, integrity or availability of a component or the entire technology infrastructure or information that is processed, stored or transmitted; that may represent a loss, alteration or misplacement of information; or that constitutes a violation or an imminent threat of violation of the security policies, security procedures or acceptable use policies; that may result in interruption of the service or in damage or loss to the customers of the affected Entity, to the general public, to its counterparties or to the Entity itself".	CNBV defines an incident as: "Any event, internal or external, that: compromises the confidentiality, integrity, or availability of information; vulnerates the technology infrastructure compromising the information that it processes, stores or transmits; or constitutes a violation of information security policies and procedures".

Table 4. Mexico: Cyber Incidents Reporting Regimes (concluded)

	Banxico	CNBV
What data is collected regarding a cyber incident?	Banxico requires financial entities to report the following data during an incident: • Date of incident • Financial institution involved • Breach description • Services affected and financial loss	CNBV requires financial entities to report the following data during an incident: • Date of incident • Duration of incident • Description • Impact assessment to systems, networks, protocols, services, customers, reputation, and financial loss • Amount recovered • Reports to other authorities Number of records exposed • Threat vector, vulnerabilities exploited and malware signatures • Containment actions taken • Results of recovery actions and any other information shared by entities
Has the authority established (a) a taxonomy of cyber incident (to designate them); (b) a categorization of their severity to measure their importance; and (c) a methodology for determining the materiality (i.e., the impact and severity) of a cyber incident that is used in cyber incident reporting?	Banxico and CNBV categorize the severity of an incident according to the following criteria, as set out in the Bases of Coordination: (i) It could represent an impact on: • More than one Entity; • Customers of the Entities; • The stability of the financial system, or, • To central payment systems, clearing houses or central securities depositories; or (ii) Encompasses the following features: • Generates economic loss, loss of information or interruption of the services of the Entity in question; • Its mode of operation can be replicated in other entities; • May represent a high reputational risk for the Entities or other participants in the financial system, or, • May generate public distrust.	
Does the authority issue a cyber incident reporting template to its supervised entities?	Yes	Yes
Channel of communication?	Email	Email
Does the authority create a cybersecurity risk summary/trend report or dashboard based on the data collected?	Yes. CNBV coordinates with Banxico to publish a summary of incidents by year on the central bank's website	

C. Recommendations

84. Banxico should work with the financial sector to develop and operationalize a cyber information and intelligence sharing network. Banxico would benefit in taking a structured approach to develop this network, engaging closely with the industry, to design the model and its operations. This should include:

- Drafting a Terms of Reference and Rulebook for its participants.
- Developing an operational platform (e.g., MISP) and creating a CISO network for in-person meetings to foster trust and sharing.
- Detailing the types of strategic, operational, and tactical information and intelligence to be shared.
- Setting out the principles for sharing and analyzing information.

This network should include a broad range of financial entities and exclude supervisors and regulators to address the industry concerns around sharing freely and without any potential supervisory repercussions, whilst still providing authorities with key information in the case that a cyber threat could become systemic.

85. CNBV should develop and document crisis communication protocols, setting out the roles and responsibilities of all the relevant stakeholders during an incident, as well as the procedures to manage an incident, whether domestic or international.

CYBER DETERRENCE

86. In Mexico, there are several laws and codes in place that set out the different types of cybercrime:

- The *Federal Penal Code* defines the crimes of federal jurisdiction, including "Disclosure of secrets and illicit access to computer systems and equipment."
- *State Penal Codes* establish crimes of local jurisdictions, including, in some cases, those related to cybercrimes.
- The laws on financial entities, such as the *Credit Institutions Law,* define crimes of the federal jurisdiction, that are committed against such entities, including, those related to cybercrimes.
- The *Organic Law of the Judicial Power of the Federation* establishes the rules to determine the cases when the investigation, prosecution, and punishment of crimes, including those related to cybercrimes, will be of the federal jurisdiction. In all other cases, any cybercrime will be of the local jurisdiction.
- The *National Code of Criminal Procedures* establishes the rules that must be observed in the investigation, prosecution, and punishment of crimes, including those related to cybercrimes.

87. To overcome a fragmentation in the different laws regarding cybercrime, the authorities are considering a Cybersecurity Law. It aims to legislate cybercrimes at the federal level. Although cyber deterrence is outside of the remit of Banxico and CNBV, there is a role for both financial authorities regarding cybercrime in the financial sector.

88. Building strong domestic capabilities and enhanced coordination of investigation and enforcement against cyber-attacks would strengthen deterrence. Financial authorities and law enforcement and prosecution agencies working together would strengthen the prevention of cybercrimes and bolster law enforcement action when attacks do occur. In Mexico, the Bases of Coordination sets out the protocol for cyber deterrence, investigation, and prosecution of cybercriminals on a federal level.

89. Clause 7 of the Bases of Coordination establishes that the FGR is responsible for investigating cybercrimes on financial entities based on forensic investigations and thereafter prosecuting cybercriminals. The FGR should collaborate with the financial authorities and entities through the Office of the Special Attorney for Federal Crimes Investigation under the structure preceding the FGR (Subprocuraduría Especializada en Investigación de Delitos Federales—SEIDF). However, there are some key challenges:

- Following a cyber incident, financial entities must formally file a criminal complaint with the FGR so that it can initiate an investigation; however, financial entities are reluctant to do so, as it may lead to the confiscation of key servers and hardware, which may hinder the entities' operations.
- Investigators and prosecutors lack the technical expertise to analyze the crime and forensic evidence.
- Crimes surrounding cybercrime are not clearly defined in law, due to the fragmentation across the different laws.
- There is a lack of guidance for financial entities on how to store, handle and administer evidence to facilitate investigations.

90. Banxico and CNBV could take steps to propose working with law enforcement agencies and the FGR, on further collaboration so that the overall process for forensic investigation in the financial sector and criminal prosecution can be effectively carried out by:

- Issuing guidance for financial entities on how to store, handle and administer evidence to facilitate investigations.
- Fostering the development of guidance by the FGR for financial entities on how to file a complaint and collaborate on the investigation.
- Raising awareness amongst law enforcement agencies and the FGR on the importance of effective investigations of cyber incidents in the financial sector.