INTERNATIONAL MONETARY FUND

IMF Country Report No. 25/231

CANADA

FINANCIAL SECTOR ASSESSMENT PROGRAM

August 2025

TECHNICAL NOTE ON CYBER RESILIENCE OF THE FINANCIAL SECTOR

This Technical Note on Cyber Resilience of the Financial Sector was prepared by a staff team of the International Monetary Fund. It is based on the information available at the time it was completed on July 22, 2025.

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

International Monetary Fund
Washington, D.C.

INTERNATIONAL MONETARY FUND

CANADA

FINANCIAL SECTOR ASSESSMENT PROGRAM

July 22, 2025

TECHNICAL NOTE

CYBER RESILIENCE OF THE FINANCIAL SECTOR

Prepared By
Monetary and Capital Markets Department

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

CONTENTS

Glossary

AMF	Autorité des Marchés Financiers
BCFSA	British Columbia Financial Services Authority
BCSC	British Columbia Securities Commission
BOC	Bank of Canada
CAR	Core Assurance Reviews
CATTIC	Cyber and Technology Threat Intelligence Centre
CCP	Central Counterparty
CCCS	Canadian Center for Cyber Security
CCSPA	Critical Cyber Systems Protection Act
CCTX	Canadian Cyber Threat Exchange
CDIC	Canada Deposit Insurance Corporation
CFACT	Canadian Financial Authorities Cyber & Technology Committee
CFRG	Canadian Financial Sector Resiliency Group
CIRO	Canadian Investment Regulatory Organization
CISO	Chief Information Security Officer
CPMI	Committee on Payments and Market Infrastructure
CSA	Canadian Securities Administrators
CSD	Central Securities Depository
CSTAC	Canadian Securities Telecommunications Advisory Committee
CUPSA	Credit Union Prudential Supervisors Association
DoF	Department of Finance
FI	Financial Institution
FIRE	Format for Incident Reporting Exchange
FISC	Financial Institution Supervisory Committee
FMI	Financial Market Infrastructure
FRFI	Federally Regulated Financial Institutions
FSB	Financial Stability Board
FS-ISAC	Financial Services Information Sharing and Analysis Center
GTL	Generic Threat Landscape
I-CRT	Intelligence Led Cyber Resilience Testing
ICMAC	Idiosyncratic Crisis Management Advisory Committee
ICT	Information and Communication Technology
IMF	The International Monetary Fund
IOSCO	International Organization of Securities Commissions
ISO	International Organization for Standardization
IT	Information Technology
MCN	Ministère de la Cybersécurité et du Numérique
MDCCG	Market Disruption and Cybersecurity Coordination Group
NSS	National Security Sector
ORAC	Oversight Risk Advisory Committee
OSC	Ontario Securities Commission

OSFI	Office of the Superintendent of Financial Institutions
PCSA	Payment Clearing and Settlement Act
PFMI	CPMI-IOSCO Principles for Financial Market Infrastructures
PRFI	Provincially Regulated Financial Institutions
RBS	Risk-based Supervision
RCMP	Royal Canadian Mounted Police
SAC	Senior Advisory Committee
TIBER-EU	Threat Intelligence Based Ethical Red-teaming
TRD	Technology Risk Division
TLPT	Threat-Led Penetration Testing
TTP	Tactics, Techniques and Procedures

EXECUTIVE SUMMARY

Cyber risk is highly relevant to the financial sector and financial stability of Canada. According to the Canadian Centre for Cyber Security (CCCS), in 2021, 23.9 percent of finance and insurance enterprises were impacted by cyber security incidents, placing Finance into the top four of the Critical Infrastructure Sectors being targeted by cyber actors. Cyber-attacks on the financial sector have tripled from 2022 to 2023 and these cyber-attacks against Canadian financial institutions (FIs) are increasing in both frequency and sophistication.

Disruptive technologies bring new opportunities and new threats. The CCCS has identified three technological trends as having the potential to disrupt their respective fields: digital assets and decentralized finance, machine learning, and quantum computing. Digital assets, such as cryptocurrencies and decentralized finance, are both targets and tools for cyber threat actors to enable malicious cyber threat activity. Machine learning automations can be exploited to launch large-scale fraud campaigns. And quantum computing has the potential to threaten the current systems of maintaining trust and confidentiality online. All these factors accentuate the need for a strong ecosystem, with forward-thinking strategies, robust regulation and supervision, and effective coordination between all stakeholders that operate and oversee the interconnected financial system.

Canada has a mature cyber ecosystem, with a broad range of stakeholders coordinating and cooperating effectively to ensure the cybersecurity of the Canadian financial system. The different stakeholders—both public and private—have made significant strides in building capacity throughout the industry and have built strong public-private structures to ensure free-flowing information and initiatives between all parties. Furthermore, the structures in place play a variety of different but crucial roles—policymaking, supervisory and operational. In addition, Canada benefits from Five Eyes membership, which gives it access to intelligence from across the Five Eyes network and has the CCCS, which is an outward looking institution, designed to work with the private sector to support the cyber resilience of Canada.

Notwithstanding this, there is room for further improvement, including by strengthening the overarching strategy and enhancing inter-agency coordination. Federal and provincial regulators could develop cyber strategies for their respective financial sectors, and there could be improved coordination, cooperation, and communication between all federal and provincial authorities, and an alignment in their approaches to enhance cyber resilience across the interconnected Canadian financial sector. In terms of strategy, the Bank of Canada (BOC) has developed a unique model, which focuses on strengthening the central bank's security and enhancing the sector's overall cyber resilience. In this context, the BOC has taken leadership in establishing the Canadian Financial Sector Resilience Group (CFRG), which is an important public-private partnership that facilitates operational resiliency initiatives for the critical financial sector and coordinates critical finance sector responses to systemic-level operational incidents. Furthermore, the Technology Risk Division (TRD) in the Office of the Superintendent of Financial Institutions (OSFI), which is only 3–4 years old, has made significant and noteworthy progress in maturing OSFI's cyber risk supervision.

As the challenges from cyber risk and technology advance in the coming years, the Canadian authorities should reflect on their strategic direction of travel and improve their overall governance arrangements and strategy to meet the challenges ahead. Currently, there are no provincial level cyber strategies for the financial sectors, and nor is there a joint federal cyber strategy. A cyber strategy would allow all relevant stakeholders to develop cyber resilience across the entire financial sector, with clearly defined roles and responsibilities, and a clear implementation plan. This would allow better coordination, cross-fertilization of initiatives and pooling of resources when needed. The national strategy for critical infrastructure requires different sectors, such as Finance, to establish a "sector network" to enhance coordination, cooperation, and communication within them. There would be benefit in the federal and provincial authorities in establishing or enhancing the mandates of existing structures to build such sector networks and leveraging them to develop cyber strategies in a consistent and aligned manner.

Federal and provincial authorities have a strong cyber regulatory framework, and guidelines, but they could better integrate them into their supervisory and oversight processes. On the whole, the authorities have comprehensive regulations and guidelines in place, which are largely in line with international standards. However, integrating the guidelines into the supervisory and oversight processes, would enable a more structured and systematic approach to risk-based supervision and oversight. For example, the BOC and the Canadian Securities Administrators (CSA) conduct joint oversight of systemically important FMIs based on two largely similar regulations, and it would be useful to map these two and develop a joint oversight methodology to ensure there are no gaps. Furthermore, British Columbia Financial Services Authority (BCFSA) and Québec's Autorité des Marchés Financiers (AMF) have a significant number of guidelines which contain cyber-specific requirements, and both authorities should map their respective guidelines to consolidate the cyber-specific requirements and integrate them into a supervisory manual to enable more focused and risk-based supervision.

There is also room to further strengthen supervisory practices. Federal and provincial authorities have a strong supervisory framework, with clearly defined processes, strong onsite and offsite supervision, and sound reliance on third-party assurance. However, some authorities could increase their onsite examinations, specifically on some systemically important financial entities. And the BCFSA should consider increasing its resources with regards to cyber supervision.

The authorities would benefit from deepening their analysis of the operational interconnectedness 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, and the transmission channels which could trigger financial instability via cyber-attacks. Based on this analysis, the authorities should develop a range of cyber contagion scenarios and use these to build stronger sector-wide crisis preparedness through scenario-based testing and incident response. This analysis would also allow authorities to identify whether there is a concentration risk from third-party providers.

The federal and provincial authorities have no legal and regulatory powers over third-party providers and rely on outsourcing guidelines to indirectly manage the potential risk borne

from them. Increasing their powers over such providers may enable the authorities to better manage the risk, as third-party providers may be a gateway for a systemic cyber incident, and supply chain attacks have been increasing in recent years globally. It should be noted that globally there has been a movement in some jurisdictions to give financial regulators more direct oversight over third-party providers, for example, the EU, UK and US.

Although the authorities currently have strong cyber incident reporting regimes in place, they may benefit from reviewing their existing incident reporting framework and should improve information sharing in that regard. The authorities should align their incident reporting framework further with the Financial Stability Board (FSB) (if appropriate) and improve the modalities for sharing incident information with each other, focusing on removing any legal barriers that impede this. Currently, the authorities do not share relevant cyber incident information with each other. This raises the risk that an incident in a province could materialize into a potential systemic incident, and due to a lack of information sharing, the relevant provincial and/or federal authorities may not have the requisite information to manage the incident from a financial stability perspective.

OSFI has developed a Threat Led Penetration Testing (TLPT) Framework.[1] but it should monitor its evolution and introduce further enhancements to it. As the framework is operationalized in the coming years, OSFI should include further types of tests and clear criteria for testers, which would allow FIs to conduct a range of such tests in a more economical manner and use only the most competent testers, given the risks borne from such tests. Furthermore, other authorities may use the framework as an inspiration for their own regulated entities.

Although the BOC, OSFI and CSA conduct or participate in market-wide exercises, all authorities may benefit from conducting such exercises on their respective financial sectors. This pertains to both federal and provincial authorities and the scope of the exercises could include third-party providers, other sectors and a broader suite of FIs. Conducting such exercises on a more frequent basis would enhance the authorities' capabilities to respond to a potentially systemic incident.

It would also be useful to leverage existing fora to be better prepared to manage systemic cyber incidents. Federal and provincial authorities have robust incident response protocols. However, the federal authorities would benefit from leveraging existing structures, to manage a systemic incident, with decision coordination, clearly defined incident management protocols, and a playbook of extreme but plausible scenarios that are regularly tested. It should be noted that there are strong and robust fora (e.g., the Senior Advisory Committee and Financial Institutions Supervisory Committee) that bring together all the relevant authorities at a senior level. However,

[1] A controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques and procedures of real-life threat actors. It is based on targeted threat intelligence and focuses on an entity's people, processes and technology, with minimal foreknowledge and impact on operations. (FSB Cyber Lexicon)

focusing efforts of these fora on cyber-specific scenarios would allow the authorities to be better prepared to manage a potential systemic cyber incident.

Canada has a fairly mature ecosystem for cyber threat intelligence and information sharing, but the exchange of information is often ad-hoc and not accessible to all. The authorities could benefit from catalyzing information and intelligence sharing networks within the private sectors across different provinces, and build a network of networks, that would enable the sharing of relevant strategic, operational, and tactical information of threats and vulnerabilities across the different provincial financial sectors in Canada. The authorities should conduct a legal review, to ensure that there is a fit-for-purpose information-sharing framework and no legal barrier in such information and intelligence sharing (e.g. data privacy laws and legal liability issues), which is vital for ensuring financial stability.

Table 1. Canada: Recommendations on Cyber Resilience of the Financial Sector		
Recommendations	**Timing[1]**	**Authorities**
Institutional Elements		
The federal authorities (Department of Finance (DoF), OSFI, BOC, Canada Deposit Insurance Corporation (CDIC) and CCCS) and all provincial financial authorities should establish, leveraging already existing structures, a "financial sector network" that aims to build, to the fullest extent possible, effective and efficient coordination, cooperation and communication mechanisms for cyber resilience.	I	All authorities (federal and provincial) and CCCS
The financial sector network should work closely together to develop cyber strategies for the financial sectors at the federal and provincial level.	ST	All authorities (federal and provincial) and CCCS
Regulatory Framework		
The BOC may consider updating its Expectations for cyber resilience for designated FMIs (ECR) with regards to third party risk management in light of the ongoing work of the Committee on Payments and Market Infrastructure (CPMI)- International Organization of Securities Commissions (IOSCO).	MT	BOC
The federal and provincial authorities should consider increasing their legal and regulatory powers over third-party providers.	MT	DoF, OSFI and BOC and provincial authorities
BCFSA and AMF may consider reviewing their suite of different guidelines and map the cyber-specific requirements to their cyber supervision and oversight frameworks.	ST	BCFSA and AMF
BOC and CSA members should continue to map their respective regulatory requirements and integrate them into a common oversight methodology.	ST	BOC and CSA
Supervisory Arrangements		
BCFSA and AMF should develop a cyber supervisory manual that aligns all cyber-specific requirements from their guidelines.	ST	BCFSA and AMF
BCFSA should conduct onsite examinations for cyber resilience on its most systemic PRFIs, including Central 1.	I	BCFSA
BCFSA should consider increasing its staffing and/or expertise in cyber supervision.	ST	BCFSA
CSA members and BOC should conduct an onsite examination related to cyber resilience of its regulated entities.	I	CSA and BOC

Table 1. Canada: Recommendations on Cyber Resilience of the Financial Sector (continued)		
Recommendations	**Timing[1]**	**Authorities**
The federal and provincial authorities could benefit from collectively reviewing their existing incident reporting regimes and updating them in line with the FSB's FIRE Framework. Consideration should be given on how to include third-party providers into the scope of incident reporting.	MT	All authorities (federal and provincial)
The federal authorities should undertake a legal review and take the necessary steps to facilitate the sharing of relevant incident information between federal and provincial regulators.	MT	DoF, OSFI and BOC
Financial Sector Resilience		
Federal and provincial authorities should work with their respective financial sectors to develop and operationalize cyber information and intelligence sharing networks.	ST	All authorities (federal and provincial) and CCCS
Authorities should consider how to develop a network of networks that facilitates sharing of information and intelligence between the different provincial financial sectors.	MT	All authorities (federal and provincial) and CCCS
Federal and provincial authorities should conduct a legal review (e.g. data privacy) on information and intelligence sharing between financial sector participants, to facilitate the sharing of such information without legal barriers (if feasible and permissible).	ST	All authorities (federal and provincial) and CCCS
OSFI should monitor the implementation of the I-CRT Framework and ensure that it has the right level of resources and expertise for its successful deployment.	ST	OSFI
OSFI should include, in the I-CRT Framework, clear criteria and conditions for threat intelligence and red-team testing providers.	MT	OSFI
CCCS should consider developing a Generic Threat Landscape (GTL), in close collaboration with other relevant agencies, such as the RCMP and CSE.	MT	CCCS
OSFI should consider updating its framework, with the integration of a GTL component, purple and gold team testing, and use the potential GTL report for other purposes such as developing playbooks, scenarios and conducting exercising.	MT	OSFI
The BOC and provincial regulators should consider applying the I-CRT for their own systemically important FIs.	MT	BOC, AMF, BCFSA

Table 1. Canada: Recommendations on Cyber Resilience of the Financial Sector (concluded)		
BOC, OSFI, BCFSA and AMF should conduct more regular cyber simulation exercises with other authorities and a broader selection of financial entities (e.g., banks, FMIs, insurance companies), and including third-party providers.	ST	BOC, OSFI, BCFSA and AMF
The financial sector network should work together in sharing their experiences of exercises.	MT	All authorities (federal and provincial) and CCCS
The federal authorities (e.g. Finance Canada, BOC, OSFI and CDIC) should consider leveraging existing structures (e.g. FISC, CFRG, SAC, etc.) to put in place a process to manage a systemic cyber incident, with decision coordination, clearly defined criteria and threshold of systemic cyber incidents, and with a clear playbook of cyber scenarios, that are regularly tested.	I	DoF, BOC, OSFI, CDIC and CCCS
The AMF and BCFSA should develop and document a sector-wide crisis management and coordination plan.	ST	BCFSA and AMF
The authorities should collect information and data of third-party providers and the technology being used by financial entities and use this data to conduct analysis of how the financial sector is operationally interconnected.	ST	All authorities (federal and provincial)

[1] I Immediate (within 1 year); ST Short Term (within 1–2 years); MT Medium Term (within 3–5 years).

INTRODUCTION[2]

A. Background: Cyber Risk as a Financial Stability Concern

1. According to the CCCS National Cyber Threat Assessment (2023–24), ransomware is a persistent threat to Canadian organizations. Due to its impact on an organization's ability to function, ransomware is almost certainly the most disruptive form of cybercrime facing Canadians. Second, critical infrastructure is increasingly at risk from cyber threat activity. Cybercriminals exploit critical infrastructure because downtime can be harmful to their industrial processes and the customers they serve. Third, cyber threat actors are attempting to influence Canadians, degrading trust in online spaces. The CCCS has observed cyber threat actors' use of misinformation, disinformation, and malinformation (MDM) evolve over the past two years. Finally, disruptive technologies bring new opportunities and new threats. Digital assets, such as cryptocurrencies and decentralized finance, are both targets and tools for cyber threat actors to enable malicious cyber threat activity. Machine learning has become commonplace in consumer services and data analysis, but cyber threat actors can deceive and exploit this technology.

2. 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 vulnerabilities, supply chain attacks, ransomware attacks, and distributed denial-of-service attacks. Additionally, non-malicious incidents like accidental data disclosures and configuration, implementation, or processing errors continue to be an important source of cyber risk.

3. The Canadian government has stepped up its efforts to support the digital economy by publishing its National Cyber Security Strategy (2019–24). It accentuates the need for a cyber-resilient economy. The Strategy defines three goals to achieve its vision of security and prosperity in the digital age: (i) Secure and Resilient Canadian Systems: with enhanced capabilities and in collaboration with partners, the Government of Canada aims to better protect Canadians from cybercrime, respond to evolving threats, and help defend critical government and private sector systems; (ii) An Innovative and Adaptive Cyber Ecosystem: The Government of Canada aims to support advanced research, foster digital innovation, and develop cyber skills and knowledge to position Canada as a global leader in cyber security; and (iii) Effective Leadership, Governance and Collaboration: In collaboration with provinces, territories, and the private sector, the federal government aims to take a leadership role to advance cyber security in Canada, and will, in coordination with allies, work to shape the international cyber security environment in Canada's favor.

[2] This Technical Note is prepared by Emran Islam, Senior Financial Sector Expert at the IMF's Monetary and Capital Markets Department. The FSAP team thanks the authorities for the constructive dialogue and the many insights that they have shared.

4. Concurrently, the Canadian financial authorities 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. 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.

B. Review Scope: Banks, Securities, Insurance, and Financial Market Infrastructures

5. This technical note reviews key elements of the cyber regulatory and supervisory framework for the financial sector in Canada. This includes: (i) the role and practices of the Canadian 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) interconnectedness and financial stability; (v) cyber risk related information and intelligence sharing; and (vi) cyber incident reporting, monitoring, response, and recovery. This review is limited to the framework for financial entities that fall within the mandate of OSFI and the BOC; the approach of the provincial authorities of Québec (AMF)[3] and British Columbia (BCFSA); and members of the CSA[4] with regards to FMI cyber regulation and supervision. Québec and British Columbia were included in the FSAP review of cyber resilience as examples of provincial oversight frameworks; however, other provinces not included in this review, may have similar, but different functions that fall outside the scope of this report. Recommendations made pertain to those authorities in scope of this review. However, when applicable, the recommendations that apply to better coordination between federal and provincial regulators can be considered more widely.

6. The FSAP team collected information from several sources. These include questionnaire answers provided by OSFI, BOC, AMF, BCFSA, CSA, British Columbia Securities Commission (BCSC) and OSC, interviews with all the authorities, DoF, CCCS, CDIC, Public Safety Canada, and private sector participants, the study of relevant national laws and reports published by the authorities, as well as documentation of their work.

7. 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 FSAP team used internationally recognized regulatory good practice as

[3] As the AMF is an integrated regulatory authority, all references to AMF within this technical note exclude securities oversight activities. Since the AMF is a member of the CSA, the AMF's securities oversight activities are included in the references to the CSA.

[4] Members of the CSA include: Alberta Securities Commission, BCSC, Manitoba Securities Commission, New Brunswick Financial and Consumer Services Commission, Office of the Superintendent of Securities Service Newfoundland and Labrador, Office of the Superintendent of Securities (Northwest Territories), Nova Scotia Securities Commission, Office of the Superintendent of Securities Nunavut, Ontario Securities Commission (OSC), Financial and Consumer Services Division (Prince Edward Island), AMF, Financial and Consumer Affairs Authority of Saskatchewan and Office of the Yukon Superintendent of Securities. For the purposes of this Technical Note, only AMF and BCSC were independently assessed.

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"; the G7 "Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector"; the "Basel Principles for Operational Resilience"; and the revised "Principles for Sound Management of Operational Risk". The basis of the review in the case of FMIs was the CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures.

INSTITUTIONAL ELEMENTS

A. Institutional and Regulatory Arrangements

8. Canada has a strong and mature ecosystem of financial authorities, governmental agencies and public-private coordination bodies with regard to cybersecurity and cyber resilience. Given the complex setup of the Canadian system, with federal and provincial structures, Canada has a range of institutions that play a pivotal role in ensuring security at all levels and across different sectors. This section discusses the roles of the most significant institutions, the regulatory arrangements, the overall cyber strategy of Canada—nationally and for the financial sector—and the effectiveness of the institutional arrangements.

Office of the Superintendent of Financial Institutions

9. OSFI regulates and supervises federally regulated financial institutions (FRFIs), which includes all banks and federally regulated trust and loan companies and insurers. OSFI's mandate is to contribute to public confidence in the Canadian financial system by regulating and supervising approximately 400 FRFIs and 1200 federally regulated pension plans (FRPPs). As part of this, OSFI expects that FRFIs adequately identify and manage technology and cyber threats and risks to support their operational resilience.

10. OSFI's response to cyber and technology risk are led by the TRD—a specialist group supporting the Supervision Sector at OSFI. TRD works closely with Supervision in developing plans and strategies to advance OSFI's mandate around technology and cyber risk management. TRD's core pillars are: Supervision, Reviews and Monitoring (SRM); Incident Response Management (IRM); Policy, Instruments and Tools (PIT); Data Driven Intelligence (DDI); and External and Internal Stakeholder Affairs (SHA). In order to deliver its plans in these areas, TRD has developed a 3-year build plan, which focuses on: enhancing supervisory processes, implementing the testing framework, enhancing incident response and structuring and automating data and key reports.

11. Recognizing the importance of emerging cyber and technology risk, the Cyber and Technology Threat Intelligence Centre (CATTIC) team was established in 2022 to identify and monitor macro cyber and technology threats and risks within the financial sector. Their threat risk assessments contribute to determining the prioritization and response of OSFI's top external risks in accordance with its risk appetite statement.

12. In 2023, OSFI established a National Security Sector (NSS) to support its mandate to consider if FRFIs have adequate policies and procedures to address threats and risks related to integrity and security, including foreign interference. The NSS will examine integrity and security risks, including foreign interference, that could affect FIs. It will also provide national security assessments, advice, and intelligence co-ordination within OSFI.

13. The collective functions inside OSFI will allow it to identify both traditional/commercial-level cyber risks as well as sophisticated/classified cyber threats that may affect the safety and soundness of the financial sector. OSFI can apply this threat information for the supervision of individual institutions and contribute to the sector overall. OSFI's legislative authorities allow it to take a range of supervisory actions. OSFI also works with CCCS and other partners to facilitate threat information sharing with the institutions within OSFI's oversight.

Bank of Canada

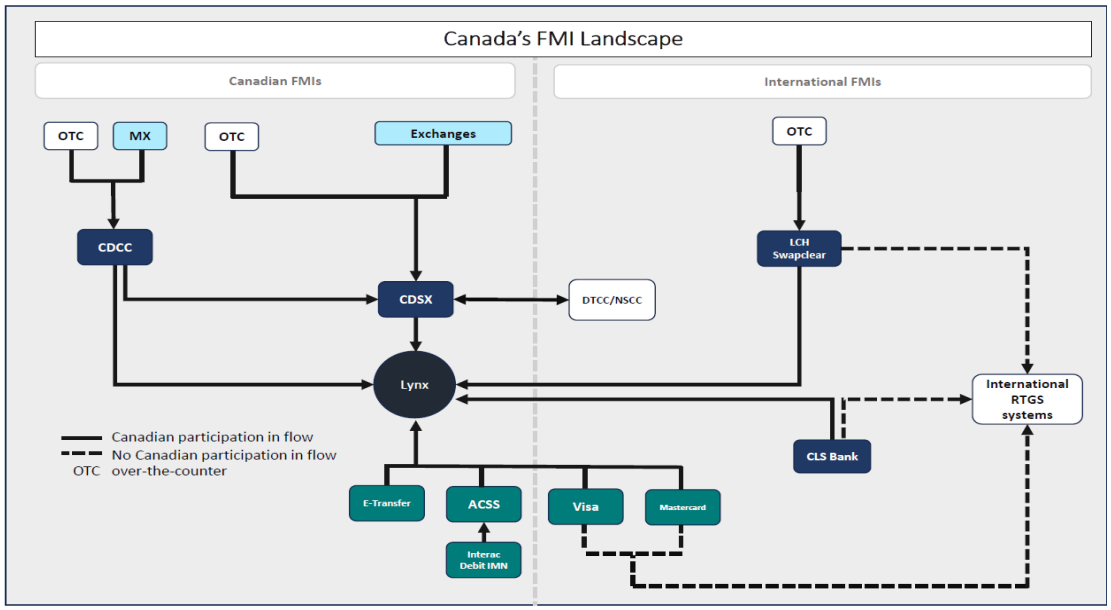
14. The BOC is the central bank, responsible for financial stability and per the Payment Clearing and Settlement Act ("PCSA"), the BOC has a mandate to ensure that clearing and settlement systems (usually called "financial market infrastructures", or "FMIs") adequately control systemic risk or payments system risk. Because cyber incidents can create systemic or payments system risk, this mandate includes cyber risk.

15. Systemically important and prominent payment systems are overseen by the BOC pursuant to the PCSA. The Bank and provincial securities commissions (collectively, the Canadian Securities Administrators, or "CSA") jointly oversee systemically important Securities Settlement Systems (SSS), Central Counterparties (CCPs) and Central Securities Depository (CSDs).

16. In terms of public-private coordination, the BOC established the CFRG. Formerly known as Joint Operational Resilience Management (JORM) Program, the CFRG is a public-private partnership led by the BOC that is designed to strengthen the financial sector's critical infrastructure against risks to business operations, including cyber incidents. The CFRG builds and maintains relationships with numerous external parties, which may benefit the financial sector[5]. The BOC also established the Resiliency of the Wholesale Payment System (RWPS), which is a public-private partnership led by the BOC to promote stability in Canada's financial system. RWPS's mandate focuses on enhancing the collective cyber resilience of the wholesale payment system by increasing and exercising cyber security capabilities related to: prevention and detection; coordination and response; and recovery from cyber incidents. Furthermore, the BOC has established the Canadian Financial Authorities Cyber & Technology Committee (CFACT), which brings together all the federal financial authorities.

[5] Government of Canada and its departments; Provincial Securities Regulators (AMF); Canadian Security Intelligence Service (CSIS); Public Safety Canada; Royal Canadian Mounted Police (RCMP); Canadian Bankers Association (CBA); Canadian Financial Services Cyber Security Governance Council (CFS-CGC); Financial Services Information Sharing and Analysis Centre (FS-ISAC); CCTX; National Critical Infrastructure members (Energy, Telecommunications, etc.); and a range of critical private sector organizations.

Figure 1. Canada: Overview of Payment and Settlement Systems



Source:

17. The CFRG consults with external critical infrastructure sector partners, as required, to identify areas of engagement on resilience initiatives and crisis coordination. The CFRG has adopted terms of reference, a mandate as well as a governance structure comprised of executive sponsors, a steering committee, a coordination directorate, and a secretariat. There is currently no multipartite agreement between the CFRG members governing the collaboration or information exchange between parties.

Department of Finance

18. The DoF has the overall responsibility for the financial sector. DoF supports the Minister's policy and legislative authorities for the financial sector. The DoF also acts as the main point of contact within the federal government for issues pertaining to the sector. The DoF does not supervise financial institutions and is largely responsible for cybersecurity policymaking for the financial sector at the federal level and leads the Senior Advisory Committee (SAC).

19. Bill C-26, An Act Respecting Cyber Security, was introduced in the House of Commons in June 2022. Part II of the Bill enacts the Critical Cyber Systems Protection Act (CCSPA). Bill C-26 is currently at third reading in the Senate and has been sent back to the House of Commons. Public Safety Canada is the lead department for the federal government in cybersecurity and the lead for the larger Bill, with the DoF leading primarily on the financial sector. The purpose of the CCSPA is to protect the critical cyber systems that underpin Canada's critical infrastructure in four federally regulated sectors: finance[6], telecommunications, energy, and transportation.

[6] Provincial regulators are responsible for the oversight of securities' activities.

Canada Deposit Insurance Corporation

20. CDIC's mandate is to provide deposit insurance, act as resolution authority for its members, and promote the stability of Canada's financial system, including if a failure happens as a consequence of a cyber incident. Being resolution-ready involves having the necessary planning, processes, tools, systems, and financial capacity, as well as the right people in place to allow CDIC to resolve a member institution if necessary.

21. CDIC focuses its planning on ensuring resolution readiness. Per the Resolution Planning By-law and CDIC Resolution Plan Guidance for DSIBs, CDIC requires DSIBs to identify reliance on key systems, IT services, and third party providers, to assess the ability to ensure the continuity of an institution's core business and critical functions in a resolution event.

Public Safety Canada

22. Public Safety Canada spearheads the effort to protect the safety and security of Canadians both at home and abroad, by coordinating the activities of federal departments and agencies tasked with protecting Canadians and their communities, businesses and interests. Public Safety is also responsible for developing policies and providing advice to the Minister of Public Safety and Emergency Preparedness. The preservation of national security is a multi-faceted endeavor that requires cooperation across a diverse range of initiatives and programs. Public Safety Canada functions as a centralized hub for coordinating work in counterterrorism, critical infrastructure, and cyber security.

Canadian Centre for Cyber Security

23. The Communications Security Establishment (CSE) is the national cryptologic agency, providing the Government of Canada with information technology security and foreign signals intelligence. As part of the CSE, CCCS is the technical authority for cyber security and information assurance. While CSE does not have a mandate with regards to cyber risk specifically, it carries out activities in support of the information assurance aspect of the CSE Act mandate. Specifically, CSE acquires, uses, and analyzes information from the global information infrastructure, or from other sources, to provide advice, guidance, and services to help protect electronic information and information infrastructures designated as being of importance to the Government of Canada.

24. The CCCS is not a regulatory body, but it is the government agency responsible for addressing cyber security incidents and working with Canadian businesses to strengthen their cyber security. The essential aspect of the upcoming Bill C-26 CCSPA is mandatory reporting of cyber security incidents to CSE and CCCS. The CCSPA would only apply to designated operators in the federally regulated finance, energy, telecommunications, and transportation sectors. CSE would leverage its existing mandate under the CSE Act for cyber security and information assurance to provide technical advice and guidance. CSE and CCCS would not assess compliance with the regulatory obligations and its advice would never be binding.

Royal Canadian Mounted Police (RCMP)

25. The RCMP Federal Policing has jurisdiction over all federal laws throughout all Canadian provinces and territories (e.g., the Criminal Code, the Controlled Drugs and Substances Act) and maintains a significant presence across Regions (Pacific, Northwest, Central and Eastern) to enforce federal mandates, and in doing so, works directly with local law enforcement.

26. RCMP Federal Policing Criminal Operations (FPCO) Cybercrime program has a mandate to investigate criminal offences related to cybercrime that fall under the Federal Policing mandate, focusing its investigative efforts on addressing the highest levels of cyber-criminality that cause significant economic or cross-jurisdictional impact to Canadians and international partners. Currently, the RCMP defines cybercrime as any crime where a cyber element (that is, the internet and information technologies such as computers, tablets or smart phones) has a substantial role in the commission of a criminal offence. The RCMP's FPCO Cybercrime program works closely with domestic and international partners to identify, disrupt, prosecute, and prevent the most significant threats that make up the cybercrime ecosystem. This includes investigating high-value threat actors and the digital infrastructure they use to facilitate sophisticated crimes, such as malware, ransomware, espionage, foreign interference, as well as attacks against government institutions, key business assets, and critical infrastructure of national importance.

27. The National Cybercrime Coordination Centre (NC3) and Canadian Anti-Fraud Centre (CAFC) are responsible for receiving, coordinating and deconflicting fraud and cybercrime reporting with Canadian and international police of jurisdiction. The NC3 was established in 2018 and receives cybercrime reporting through other Canadian and international police partners. It has a national leadership role for ensuring connectivity, specialized support and coordination of law enforcement cybercrime activities in prevention, disruption, and response/apprehension related areas—both domestically and internationally. The CAFC receives cybercrime and fraud reports from both individuals and organizations, enriches reporting with available intelligence, and connects this information with national and international investigations.

28. The RCMP has many partnership outreach efforts that actively engage representatives from the Canadian finance sector to share information and intelligence, **promote the reporting of cybercrime to law enforcement and coordinate efforts to support investigation, with the police of jurisdiction (RCMP or other) that may contribute to the prosecution of cyber criminals**. Various sections of the RCMP have working relationships with the financial sector—either individually or through national associations such as the Canadian Bankers Association (CBA)—and collaborate on efforts to reduce the impact of cybercrime connected to the financial markets and infrastructure and assist in the prosecution of cybercriminals.

British Columbia

29. BCFSA supervises and regulates provincially regulated financial institutions ("PRFI")—credit unions, pension plans, insurers, and trust companies—to determine whether they are in sound financial condition and are complying with their governing laws and supervisory standards.

30. The BCSC derives its regulatory mandate under the Securities Act (British Columbia) (the B.C. Act). The B.C. Act provides the BCSC with the authority, on application, to recognize certain persons, including exchanges, quotation and trade reporting systems, clearing agencies and trade repositories.

31. In British Columbia, the following authorities are responsible for the cybersecurity of FIs: BCFSA, BCSC, OSFI, Insurance Council of British Columbia, Office of the Information and Privacy Commissioner and Consumer Protection BC.

32. Where BCFSA has information sharing agreements in place with several of these entities, they are not specific to information security but in most cases are broad enough to permit information sharing on information security issues.

33. There is no MOU or similar arrangement for sharing of information. For example, OSFI does not share cyber incident related information for banks or federally regulated insurance companies authorized to carry out business in British Columbia.

Québec

34. The AMF is the body mandated by the Government of Québec to regulate Québec's financial markets and assist consumers of financial products and services. The AMF oversees the areas of insurance, securities, derivatives, deposit institutions—other than banks—and the distribution of financial products and services. The AMF's mandate and mission are enunciated in the Act respecting the Regulation of the Financial Sector (RFSA). The AMF's role is, notably, to supervise regulated entities[7], FIs, and credits assessment agents and ensure they comply with the obligations imposed on them by law, which includes in scope IT and cybersecurity.

35. In 2021, the government of Québec created a new ministry, the Ministère de la Cybersécurité et du Numérique (MCN) to bring together technology services, **digital infrastructure expertise, and cybersecurity and cyber threat prevention.** This new ministry brings together all government activities relating to cybersecurity and digital technology, previously carried out by different organizations, in a single department. Priorities include preventing

[7] "Regulated Entities" refer to exchanges and markets, clearing agencies, self-regulatory organizations, contingency funds, and other entities the AMF has recognized, designated, authorized or exempted for the purpose of carrying on securities or derivatives activities in Québec.

cyber-attacks against the state, protecting Quebecers' public data, and enhancing digital systems already in place.

36. The MCN has the mission of leading and coordinating the Québec government's actions in the areas of cybersecurity and digital technology. It proposes to the government general policy directions in these areas, determines the sectors of activities where it intends to act as a priority, and advises the government and public bodies. It also proposes measures to increase the effectiveness of the fight against cyber-attacks and cyber threats in Québec.

37. The AMF has been exempted in large part from the application of this Act. However, while remaining independent from the MCN, the AMF collaborates on certain activities and shares cyber threat intelligence with the MCN and the cellule gouvernementale de cyberdéfense (government cyber defense unit), a community that regularly discusses cyber defense issues. The AMF is also part of the réseau d'alerte gouvernemental (government alert network), a community that provides information security respondents with access to operational-level security information. The MCN's activities do not cover private sector entities, such as those of the financial sector. On that topic specifically, the AMF is working with the CCCS and CFRG.

Canadian Securities Administrators

38. The CSA is the umbrella organization of Canada's provincial and territorial securities regulators whose objective is to improve, coordinate, and harmonize regulation of the Canadian capital markets. The CSA is not a legal entity but rather an association comprised of member provincial and territorial securities regulators, which serves as a centralized mechanism for coordination of the provincial and territorial securities regulators across Canada.

39. The securities regulators work cooperatively to adopt harmonized requirements for clearing agencies in Canada. To this end, the securities regulators conduct ongoing monitoring of clearing agencies, including regularly inspecting their operations and reviewing their proposed rules and rule changes. When applicable, this work is carried out on a coordinated basis with the BOC.

40. To operate as a clearing agency in a Canadian province or territory, clearing agencies must apply for recognition or for exemption from the requirement to be recognized under securities legislation. A clearing agency must comply with the relevant requirements of NI 24-102 Clearing Agency Requirements (NI 24-102), as well as any terms and conditions in its recognition or exemption order. NI 24-102 adopts the international standards set out in the PFMIs.

41. Overall, the Canadian financial system has a strong legal and regulatory framework for managing cyber risk but there is no regulatory power over critical service providers. Both at federal and provincial levels, the financial authorities have appropriate legal and regulatory pillars to conduct their supervision and oversight of the different types of FIs. Notwithstanding this, none of the financial authorities have any regulatory power over the critical service providers or the broader supply chain and are limited to indirect power by ensuring that FIs govern their outsourcing relationships adequately.

B. National and Financial Sector Cyber Strategy

42. Public Safety Canada is responsible for defining the national cyber strategy and national strategy for critical infrastructure. The goal of the National Strategy for Critical Infrastructure is to build a safer, more secure, and more resilient Canada. To this end, the National Strategy advances more coherent and complementary actions among federal, provincial and territorial initiatives and among the ten critical infrastructure sectors, which includes Finance. With a view to enhancing the resiliency of critical infrastructure in Canada, the objectives of the Strategy are to:

- Build partnerships;
- Implement an all-hazards risk management approach; and
- Advance the timely sharing and protection of information among partners.

43. The Strategy proposes to establish "sector networks", at the national level, for each of the critical infrastructure sectors. This approach aims to build, to the fullest extent possible, upon existing coordination and consultation mechanisms. The sector networks reflect a partnership model that will enable governments and critical infrastructure sectors to undertake the range of activities (e.g. risk assessments, plans to address risks, exercises) unique to each sector. Working with these critical infrastructure partners, each sector-specific federal department and agency should facilitate the development of sector networks to suit the needs of their stakeholders. The Strategy provides a framework for the functions of the sector networks, including:

- Promotion of timely information sharing;
- Identification of issues of national, regional or sectoral concern;
- Use of subject-matter expertise from critical infrastructure sectors to provide guidance on current and future challenges; and
- Development of tools and best practices for strengthening the resiliency of critical infrastructure across the full spectrum of prevention, mitigation, preparedness, response and recovery.

44. Public Safety Canada has also developed the 2025 National Cyber Security Strategy (the Strategy), which is predicated on three core pillars: working with partners to protect Canadians and Canadian businesses from cyber threats; making Canada a global cyber security industry leader; and detecting and disrupting cyber threat actors. The Strategy outlines two overarching principles that will guide Canada's approach to cyber security: first, it emphasizes the importance of whole-of-society partnerships to advance and strengthen Canada's cyber resilience. One way this will be done is through the establishment of the Canadian Cyber Defense Collective (CCDC), which will formalize collaboration and information sharing between the Government of Canada, provincial and territorial governments, municipalities, Indigenous

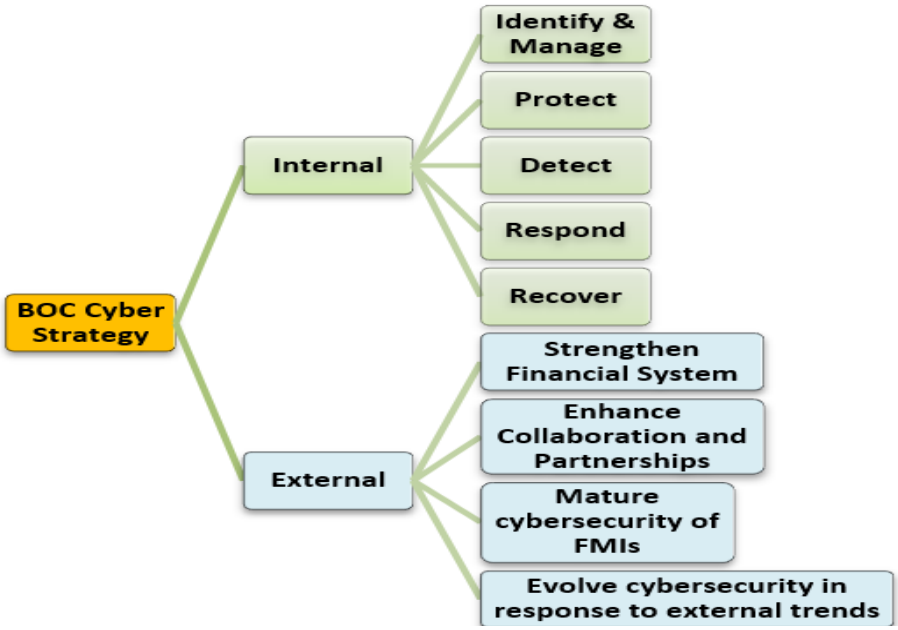
organizations, law enforcement, private industry (including the financial sector), and academia; and second, it takes an agile approach to cyber threats. Rather than a single static plan, Canada's cyber security solutions will be developed in collaboration with the CCDC and other relevant partners and stakeholders through a series of issue-specific action plans in the coming years.

45. OSFI has not developed a dedicated public cyber strategy for the institutions it regulates. However, risks posed by cyber and technology risk in the financial sector are identified in OSFI's Annual Risk Outlook, as is OSFI's response to these risks. As part of this response, TRD has developed a 3-year plan, which focuses on: enhancing supervisory processes, implementing the testing framework, enhancing incident response, and structuring and automating data and key reports. The 3-year plan is comprehensive, detailed, and demonstrates that TRD is a mature and well-established function that effectively progresses the cyber agenda at OSFI.

46. The BOC has a dedicated cyber strategy for the financial sector that falls within its mandate. Its vision is "To strengthen the cyber resilience of the Canadian financial system against an evolving threat environment", with three key goals from 2022–24: 1) Continue to integrate cyber resilience into all BOC business operations as the Bank evolves; 2) Expand financial sector resilience through collaboration and partnerships; and 3) Inspire confidence in the financial system through clear cyber security guidance within the Bank's mandate.

47. The BOC has a unique cyber strategy that is divided into two sections—an internal strategy that aims to build the cyber resilience of the central bank and an external strategy that aims to strengthen the resilience of the wider financial system. The pillars of the strategy are set out as follows, with each pillar having underlying outcomes and actions:

Figure 2. Canada: Bank of Canada Cyber Strategy



Source: IMF Staff

48. British Columbia (BCFSA) and Québec (AMF) have no dedicated cyber strategies for their financial sectors. Both authorities have focused in the last 4–5 years on building their regulatory and supervisory frameworks for cyber risk and acknowledged that developing a cyber strategy would be a useful next step to increase their focus on this risk area.

49. The BOC has a unique and effective cyber strategy, which has significantly improved the cyber resilience approach of the Canadian financial sector. The approach of combining the internal and external pillars has increased transparency across the financial sector and has led to the establishment of strong public-private structures that have bolstered the overall collaboration between the authorities and the market. Furthermore, OSFI's TRD has a focused strategy on improving its cyber supervision. In recent years, the role of BOC and OSFI have been instrumental in driving the sector towards building resilience and creating a mature Canadian ecosystem. However, as the threat landscape continuously evolves, and Canada considers how to enhance its maturity level, there may be benefit in bringing together all the relevant stakeholders to take stock of their respective roles and responsibilities and considering the next phase of collective work in a strategic manner, to further improve the overall direction of travel and the appropriate governance structures to implement the required objectives.

50. There is no joint cyber strategy for the Canadian financial sector, which has been collaboratively developed by all the relevant federal authorities. 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 a joint cyber strategy tailored to the nature, size, complexity, risk profile, and culture of the 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 other sectors upon which the financial sector depends, and with other relevant jurisdictions. A cyber strategy should clearly delineate the roles and responsibilities of the different authorities, and how they interact with each other on the issue of cyber risk. Furthermore, the cyber strategy should set out the short-, medium- and long-term vision for the financial sector, and an implementation plan to achieve the defined objectives.

51. There are no provincial level cyber strategies, developed by the relevant provincial regulator(s). The levels of maturity, skills and expertise, and resources amongst the different provinces differ, and therefore, there may be significant benefit and efficiencies in provinces aligning their own approaches, initiatives, and strategies with the federal initiatives, thereby increasing their capacities in the longer term and benefiting from pooling or leveraging expertise and resources from federal authorities.

52. To this end, it would be useful for each province to develop its own dedicated cyber strategy for its financial sector, and for there to be a "financial sector network" (leveraging the concept from the National Critical Infrastructure Strategy) between the federal and provincial authorities, that ensures a convergence in approach between all regarding developing cyber resilience across the entire Canadian financial sector. There is already a

structure, notably CFACT, which brings together federal authorities, and this could be further enhanced with additional stakeholders added to its composition.

C. Coordination Across Authorities

53. Canada has a mature cyber ecosystem, with a broad range of stakeholders—both public and private—coordinating and cooperating effectively to ensure the cybersecurity of the Canadian financial system. The DoF, Public Safety, CCCS, RCMP, OSFI and BOC have made significant strides in building capacity throughout the industry and have built strong public-private structures to ensure free-flowing information and initiatives between all parties. Furthermore, the structures in place play a variety of different but crucial roles—policymaking, supervisory and operational.

54. However, there are improvements that can be made in cooperation, coordination and communication at federal and provincial levels. For example, there appears to be an inconsistency in the involvement of the provincial authorities, with AMF participating in the CFRG, whilst BCFSA (and systemically important Central 1) being notably absent. Furthermore, at provincial levels, there are no forums or groups that bring together local regulators to work together specifically on cyber risk; although this said, some provincial regulators do participate and coordinate their efforts through CSA committees (Systemic Risk Committee, Oversight Committees, etc.). Whilst it is acknowledged that there are many agencies and authorities distributed across Canada, and this therefore makes coordination, cooperation, and communication difficult, bureaucratic, and potentially cumbersome between them all, there is the risk that gaps in cooperation, coordination, and communication could result in the ineffective management of a cyber incident with a national systemic impact, and fragmentation across provinces.

55. At the federal level, there are a number of different fora that facilitate cooperation and coordination, such as the Financial Institutions Supervisory Committee (FISC), Chaired by OSFI, SAC led by the DoF, and the CFACT led by the BOC. These fora all bring together the different federal authorities for different purposes, objectives, and mandates.

56. In terms of the public-private coordination, the CFRG has been instrumental in driving momentum, conducting exercises (intra-sector and cross-sector) and developing a crisis coordination playbook for the sector. However, discussions with the private sector and authorities have indicated that the overall function of the CFRG and other associated fora (e.g. Resiliency of Wholesale Payments System Group) could be reviewed and refreshed. There is the risk that these fora are duplicating efforts, increasing fragmentation, lacking senior level involvement, and whilst they are effective for sharing information, they lack decision making capacity. Furthermore, discussions with the private sector raised concerns that these working groups are focusing too heavily on granular operational matters, without necessarily reviewing the bigger picture and addressing the key strategic issues in the rapidly evolving threat landscape.

Recommendations

57. The federal authorities (DoF, OSFI, BOC, CDIC and CCCS) and all provincial financial authorities should establish a *"financial sector network"*, that aims to build, to the fullest extent possible, effective and efficient coordination, cooperation, and communication mechanisms for cyber resilience. The financial sector network could reflect a partnership model that will enable all relevant stakeholders to develop the right structures, modalities of communication, and protocols to undertake the range of activities that will enhance the cyber resilience of the Canadian financial sector, with clearly defined roles and responsibilities, and clear governance structures for implementation. The network could build on existing structures. For instance, it could be that the CFACT is leveraged and further enhanced to achieve the concept of a financial sector network.

58. The financial sector network should work closely together to develop cyber strategies for the financial sectors at federal and provincial level, that facilitates a convergence in approach and includes:

- Promotion of timely information sharing;
- Identification of issues of national, provincial or sectoral concern;
- Improvement of public-private coordination in all areas;
- Approaches to catalyze tools and initiatives that address cyber risk and strengthen the resiliency of financial sectors across the full spectrum of prevention, mitigation, preparedness, response and recovery; and
- Sharing of best practices between all parties.

An example of such a network ("Hub and Spoke" model) can be seen in Annex 1. Other models can also be referenced, such as the UK's operating model for its Financial Sector Cyber Collaboration Centre (FSCCC) or the USA's Financial and Banking Information Infrastructure Committee (FBIIC).

REGULATORY FRAMEWORK

A. Regulation

Office of the Superintendent of Financial Institutions

59. As the prudential supervisor, OSFI has set out a range of guidelines for its supervised entities, which all contain aspects related to cyber risk management:

- Technology and Cyber Risk Management Guideline

- Technology and Cyber Security Incident Reporting Guideline
- Third-Party Risk Management Guideline
- Integrity and Security—Guideline
- Operational Risk Management and Resilience—Guideline

60. The Guideline on Technology and Cyber Risk Management (B-13) establishes OSFI's expectations related to technology and cyber risk management. It is principles-based and focuses its expectations on three domains: governance and risk management, technology operations and resilience, and cyber security. Each domain is predicated on a defined outcome: (i) Technology and cyber risks are governed through clear accountabilities and structures, and comprehensive strategies and frameworks; (ii) A technology environment that is stable, scalable, and resilient. The environment is kept current and supported by robust and sustainable technology operating and recovery processes; and (iii) A secure technology posture that maintains the confidentiality, integrity, and availability of the FRFI's technology assets. For each of these outcomes, OSFI sets out principles and practical steps to operationalize the principles[8].

61. B-13 is a comprehensive guideline and largely in line with international standards. The expectations cover all the main components of a cybersecurity regulation, and the principles are well drafted and allow sufficient flexibility to FIs to implement measures in a proportionate and robust manner.

62. Supplementing B-13, OSFI has a range of other guidelines on different risk areas, which have expectations that are synergistic with cybersecurity, and all of these are also principles-based and in line with international standards.

Bank of Canada

63. The BOC has adopted the CPMI-IOSCO Principles for Financial Market Infrastructures (PFMIs), including associated guidance, as its oversight standards. Specific to cyber risk, the BOC has issued "Expectations for Cyber Resilience for Designated FMIs" ("ECR") and "Guideline for Designated Financial Market Infrastructures: Reporting Technology and Cyber Security Incidents" ("Incident Reporting Guidelines"). These expectations are the basis of Core Assurance Reviews (CAR) on cyber risk, and non-cyber operational risk.

64. The ECR is a comprehensive set of expectations, based on the CPMI-IOSCO Guidance for cyber resilience of financial market infrastructures (Cyber Guidance). The 2016 Cyber

[8] The principles cover the following areas: Accountability and organizational structure; Technology and cyber strategy; Technology and cyber risk management framework; Technology architecture; Technology asset management; Technology project management; System Development Life Cycle; Patch management; Incident and problem management; Technology service measurement and monitoring; Disaster recovery; Confidentiality, integrity and availability of technology assets; Identify; Defend; Detect; and Respond, recover and learn.

Guidance is largely high-level and principles based, and therefore the ECR is a well-crafted document that sets out more detailed and practical steps for FMIs to operationalize the Cyber Guidance. The ECR provides a robust framework for the BOC to conduct its oversight of FMIs and covers all the major and required components for cybersecurity, namely: governance, identification, protection, detection, response and recovery, testing, situational awareness, and learning and evolving.

65. The BOC is currently considering updating the ECR with requirements pertaining to third party risk management, which would be a sensible next step given the increasing importance of supply chain risk as a driver to heighten cyber risk and the current ongoing work of CPMI-IOSCO in this topic.

Department of Finance

66. The DoF helps the Government of Canada develop and implement strong financial sector policies and legislation. It plays an important central agency role, working with other organizations to ensure that the Government's agenda is carried out, and the Minister of Finance is accountable to Parliament for ensuring that their responsibilities are fulfilled both within the Finance portfolio and with respect to the authorities assigned through legislation.

67. The CCSPA aims to establish a regulatory framework to support the improvement of baseline cyber security for services and systems that are vital to national security and public safety. The CCSPA is driven by Public Safety but aims to designate responsibility of the financial sector to the DoF. In terms of scope of application, Schedule 1 of the Act lists services and systems that are vital to Canada's national security or the public safety of Canadians. Schedule 1 includes banking systems and clearing and settlement systems.

68. Schedule 2 of the Act would define classes of operators of the vital services and systems identified in Schedule 1. Operators captured in a class would be designated operators subject to the Act. The CCSPA would require designated operators to:

- Establish a cyber security program (CSP) to ensure the protection and resilience of their critical cyber systems. The CSP must include taking steps to identify and manage their own cyber security risks and to protect their critical cyber systems;
- Have measures in place to detect cyber security incidents and to minimize the impact of such incidents on critical cyber systems;
- Take steps to manage cyber security risks associated with an operator's supply chain and/or its use of third-party products and services; and
- Respond to cyber security directions from the Government of Canada (i.e., mechanism to compel action in response to a cyber security threat or vulnerability).

69. The CCSPA would leverage regulators' expertise and relationships with entities they already regulate under existing legislation. Schedule 2 of the CCSPA would identify both the classes of designated operators as well as the regulator responsible for enforcing the CCSPA for each class. The intent is for OSFI to be designated as the appropriate regulator for banking systems; and for the BOC to be designated as the appropriate regulator for clearing and settlement systems.

70. The CCSPA would also grant new powers to the relevant regulators (i.e., OSFI for banking systems and the BOC for clearing and settlement systems). This would include, for the purpose of verifying compliance with the CCSPA, the ability to enter and conduct inspections in places to which the requirements of the Act apply. It would also include the power to issue an "order of compliance" to a designated operator, where certain thresholds are met.

71. However, it is notable that CCSPA does not give the financial authorities legal and regulatory powers over third-party service providers. Given the importance of third-party service providers to the financial system and their potential to trigger financial instability (discussed later in the section on Financial Sector Resilience), DoF, OSFI, and BOC should explore how best to strengthen their legal and regulatory powers over third-party service providers.

British Columbia (BCFSA)

72. BCFSA has issued an Information Security Guideline for B.C. regulated credit unions, insurance companies, pension plan administrators, and trust companies collectively referred to as "PRFIs". BCFSA is currently in the process of revising its Information Security Guideline for B.C. registered pension plan administrators. Finally, BCFSA has issued, for consultation, a draft incident reporting guideline for extraprovincial insurance corporations and extraprovincial trust corporations outlining expectations regarding the reporting of material information security incidents by insurance and trust corporations incorporated in other provinces, and federally regulated insurance and trust corporations, that are authorized to conduct business in B.C. ("extrapros").

73. BCFSA has issued an Outsourcing Guideline requiring regulated entities that outsource functions to third parties to ensure these service providers meet information security guidelines. Finally, BCFSA has issued a Recovery Plan Guideline which requires PRFIs to be prepared to respond to and recover from material operational changes or significant internal and external events.

74. BCFSA's Information Security Guideline is a principles-based document, which is in line with international standards. The Guideline is based on the NIST Cybersecurity Framework, with expectations set around the following core domains: Governance, Information Security Risk Management Program, Identify, Protect, Detect, Respond and Recover. The expectations are well crafted and comprehensive, and sufficiently clear for FIs. Furthermore, the expectations are principles-based, allowing firms to apply measures in a flexible and proportionate manner.

Québec (AMF)

75. Regulatory expectations established for FIs with respect to cyber risks relate to privacy, cybersecurity, third-party relationships, outsourcing and incident disclosure. These expectations apply to insurers, deposit-taking institutions, trust and loan companies, firms and representatives, securities and derivatives, market infrastructures and mortgage brokers.

76. The AMF's expectations with regards to FIs' cyber resilience are integrated in a number of different guidelines:

- Sound Commercial Practices Guideline;
- Guideline on Information and Communications Technology Risk Management;
- Outsourcing Risk Management Guideline;
- Operational Risk Management Guideline;
- Business Continuity Management (BCM) Guideline;
- Financial Crime Risk Management Guideline;
- Governance Guideline; and
- Integrated Risk Management Guideline

77. Furthermore, the AMF will publish in the coming months a new Regulation respecting the management and reporting of information security incidents by certain FIs and by credit assessment agents (CAA). The public consultation of the regulation ended on February 20, 2024, and comments from the industry were published. The regulation is presently awaiting approval from the Québec's ministère des Finances and will come into force on April 23, 2025.

78. The AMF's Guideline on Information and Communications Technology Risk Management is principles-based and in line with international standards. The Guideline covers all the major components of a robust cybersecurity framework, notably: governance, risk management, ICT security, ICT operations, outsourcing and cloud computing, and change projects and programs. The expectations are sufficiently flexible, allowing firms to implement them in a proportionate and robust manner in line with their specific business models and capacities.

Canadian Securities Administrators

79. The securities regulators work cooperatively to adopt harmonized requirements for, amongst others, clearing agencies in Canada. To operate as a clearing agency in a Canadian province or territory, clearing agencies must apply for recognition or for exemption from the requirement to be recognized under securities legislation. A clearing agency must comply with the relevant requirements of NI 24-102 Clearing Agency Requirements (NI 24-102), as well as any terms

and conditions in its recognition or exemption order. NI 24-102 adopts the international standards set out in the PFMIs. Any entity that applies to carry on business as a clearing agency in one of the Canadian provinces or territories must demonstrate that its systems and technology, risk management, operations, and outsourcing arrangements meet the minimum requirements of NI 24-102 with respect to its systems, which includes cybersecurity risk.

80. Cyber resilience is listed in the broader operational risk management requirements of NI 24-102 which sets out requirements clearing agencies must adhere to for systems, business continuity planning and outsourcing, including:

- The implementation of adequate internal controls over the systems;
- The implementation of adequate cyber resilience and information technology general controls, including, controls relating to information systems operations, information security, change management, problem management, network support, and system software support;
- Annual capacity stress testing and capacity estimates;
- Prompt notification of incidents (failures, malfunctions, delays, security incidents, etc.) to regulatory authorities;
- Keeping a record of any incidents;
- Annual vulnerability assessments;
- Annual system reviews performed by external auditors;
- The implementation and testing of business continuity plans, including disaster recovery plans; and
- The participation in industry-wide business continuity tests.

81. In addition to the regulatory framework referred to above, the securities regulators have issued the following guidance on cybersecurity to further clarify expectations of clearing agencies:

- CSA Staff Notice 11-338 CSA Market Disruption Coordination Plan (dated October 18, 2018).
- CSA Staff Notice 11-336 Summary of CSA Roundtable on Response to Cyber Security Incidents (dated April 6, 2017).
- CSA Staff Notice 11-332 Cyber Security (date September 17, 2016), providing an update on the CSA Staff Notice 11-326.
- CSA Staff Notice 11-326 Cyber Security (dated September 26, 2013).

82. The requirements set out in NI 24-102 Clearing Agency Requirements (NI 24-102) are comprehensive and cover all the appropriate controls for cybersecurity, in line with international standards.

83. Overall, the federal and provincial authorities reviewed in the scope of this Technical Note have a broad and comprehensive suite of regulation and guidelines to address cyber risk, and the Cyber and Technology related guidelines are largely aligned across both federal and provincial authorities. The guidelines are well drafted, in line with international standards and broadly principles-based, allowing for a risk-based supervisory approach. Notwithstanding this, there are a significant number of Guidelines that are applicable to FIs. Although these are discrete and cover different topics in their own right, they all have some cyber dimension to them.

84. Across five authorities (OSFI, BOC, BCFSA, AMF, and CSA), there are 21 guidelines, regulations, or guidance, which include expectations or requirements around cyber risk management. The significant number of guidelines may make supervision challenging, as supervisors will need to take into consideration multiple requirements across several guidelines and therefore find it difficult to apply a risk-based and proportionate approach.

85. In this regard, it may be useful for the BCFSA and AMF to review their guidelines, rationalize them and map all of the cyber-specific requirements to an integrated and standardized approach for their cyber supervision. Although OSFI has done this, other authorities have yet to do so. Secondly, the BOC's ECR and NI 24-102 Clearing Agency Requirements (NI 24-102) are largely aligned, but given they are both used to jointly oversee CDS and CDCC, it would be useful to map the requirements for these two regulations and ensure that they are integrated into a common, standardized methodology for oversight. CSA, BCSC, AMF, OSC, and BOC have indicated that this is an ongoing task, and it would be recommended that they continue to this.

86. Currently, none of the federal nor provincial authorities have any legal or regulatory powers over third-party providers. All of the authorities rely on outsourcing guidelines to manage risk borne from such providers, and there is the risk that due to concentration risk amongst some providers, a cyber incident at a provider could trigger financial instability. Therefore, all authorities should explore how to increase their legal and regulatory powers overs such providers.

Recommendations

- The BOC may consider updating its ECR with regards to third party risk management in light of the ongoing work of the CPMI-IOSCO.
- The federal and provincial authorities should explore mechanisms that will increase their legal and regulatory powers over third-party providers. As a reference, the authorities may look at other examples of legal and regulatory frameworks, such as the Euro Area's Digital Operational Resilience Act (DORA) and the UK's Financial Services and Markets Act (FSM) Act 2023, which granted HM Treasury new powers to designate service providers as critical third-party providers

(CTPs) if their failure would pose a threat to financial stability or confidence in the U.K. financial system.

- BCFSA and AMF may consider reviewing its suite of different guidelines to identify the requirements related to cyber risk management and map these requirements to its cyber supervision and oversight framework, to enable a more structured and complete approach to its assessment processes.

- BOC and CSA members should continue to map their respective cyber specific regulatory requirements, to ensure that they can be integrated into a common oversight methodology and allow a standardized approach for their cooperative FMI oversight.

SUPERVISORY ARRANGEMENT

A. Supervisory Priorities and Processes

Office of the Superintendent of Financial Institutions

87. OSFI has a strong supervisory framework with regard to cyber risk. OSFI combines onsite, offsite, and thematic review in a risk-based approach and uses other instruments, such as the Cyber Security Self-Assessment tool and independent assurance, to supplement its approach. The process for onsite examinations is sufficiently detailed and structured, and OSFI has conducted a substantial number of onsite examinations in the last three years, relative to its peer jurisdictions. The review and risk rating given to FRFIs on operational resilience (which includes cyber risk) is well integrated into the overall risk rating and tiering for the FRFIs, and therefore cyber risk is well integrated into the overall supervisory framework. Finally, reports on onsite examinations and subsequent findings are well drafted and communicated to FRFIs. TRD has made significant progress in a short time to build a strong degree of maturity to OSFI's cyber supervision, and its 3-year plan going forward promises to continue this maturity with more integrated processes and automated tools.

88. OSFI's Supervisory Framework applies proportionality in its supervisory approach based on risk, size, and complexity of the institution. Each institution is given a risk rating based on its ability to manage the following risks: business risk; financial resilience; operational resilience; and risk governance. The operational resilience category includes an assessment of technology, cyber, and operational risks.

89. OSFI uses a range of policy instruments and tools as part of its supervisory process on cyber security and technology. These include, amongst others, the Cyber Security Self-Assessment tool which was originally published in 2013 and updated in August 2021. This tool assists FRFIs to conduct self-assessments in cyber security.

90. OSFI's focus areas for supervisory work (onsite examination or offsite monitoring) are driven by risks that are observed either for a specific FRFI or the sector. For example, OSFI conducted cloud computing reviews in 2020/2021 across all the large banks because of the rapid adoption of cloud services. OSFI may also choose to do a review for a specific area of risk or concern at an FRFI, for example, on incident response or disaster recovery, etc.

91. The conduct of OSFI onsite examinations involves:

- Conducting discovery meetings with key stakeholders to understand relevant processes and controls to inform scope, coverage, and identify material to be supplied by the institutions.
- Requesting and reviewing detailed artifacts prior to the start of the examination to understand the governance structures in place, control environment, risk assessment, monitoring and reporting, and controls implemented by the institutions. Following the review of these documents, multiple meetings are held with key stakeholders of the institutions to clarify OSFI's understanding of the processes and controls implemented. Additional artifacts are requested to assess and substantiate the effectiveness and sustainability of the processes and controls in place.
- Walkthroughs and demonstrations of processes and tools implemented by the institutions are also requested as needed to clarify OSFI's understanding.
- During the course of a typical review, OSFI conducts 10–15 meetings and reviews 100+ documents provided by institutions.

92. Control effectiveness testing is part of the onsite reviews. Controls included in reviews are informed by OSFI's assessment of the risks the institution faces gathered though monitoring, analysis of incidents reported by the institution and peers, collaboration with industry surveillance groups, emerging risks impacting the industry, and in consultation with lead supervisors. Over the past few years, OSFI has focused reviews on foundational controls related to governance and oversight, risk management, cloud computing as institutions were developing and delivering on strategies to increase their cloud presence.

93. Monitoring or offsite processes are less intrusive on institutions. They aim at monitoring technology and cyber risks by requesting and reviewing risk management artifacts produced by institutions followed by meetings or follow-up questions using a risk-based approach. These include architectural documentation, risk management framework, policies and standards, risk management, and board reports with key technology and cyber related KPIs and KRIs.

94. In the last three years, OSFI has conducted 35 technology and cyber related onsite examinations, some of which also include examinations following cyber incidents reported by FRFIs. OSFI conducts thematic examinations leveraging its review process and monitoring process which can result in supervisory letters with recommendations. For example, thematic monitoring of Business Continuity (BCP) and Disaster Recovery (DRP) processes of small and medium size

institutions resulted in supervisory letters with recommendations and an industry letter. Thematic monitoring of Cloud and Cyber risks for selected FRFIs and Technology Currency Management processes resulted in a comparative analysis shared with the targeted institutions. Finally, OSFI has developed mature Criteria Matrices, which are well drafted supervisory assessment guides (e.g. supervisory manual), that personnel can refer to when conducting onsite examinations against each topic area of the B13 Guideline.

95. OSFI's mandate is limited to assessing the quality of third-party risk management at FRFIs. OSFI does this through monitoring and onsite reviews of an institution's third-party risk management practices.

96. Reliance on independent cybersecurity attestation or other assurance can vary depending on a few factors such as the oversight provided by OSFI, whether the attestation or assurance work was commissioned by an independent party and the nature and purpose of the assessment. Limited reliance is placed on assessment and attestation led by institutions for internal purposes or for commercial purposes (e.g., SOC2 type 2). The results of such work can be used to inform OSFI's monitoring of institutions. Furthermore, limited reliance is placed on self-assessments. The results of these are validated through follow-up meetings and requests for information to verify and substantiate their content.

97. Under OSFI's methodology and approach, they do not formally define risk ratings for individual findings. However, the severity of findings influences the risk rating assigned to the institution. Priorities and area of concerns are also communicated in the annual supervisory letter to the institutions. In addition, OSFI communicates specific findings related to cyber risk back to the institution if appropriate as part of its supervisory approach.

98. OSFI follows-up on all findings and assesses the sustainability of the remediation. For institutions that have robust risk management and internal audit functions, OSFI requests that they verify and challenge the closure of the findings.

Bank of Canada

99. The Bank's oversight framework consists of oversight standards, periodic assessments, or "CAR" against those standards, regular monitoring, and approval of significant changes. The CAR on cyber risk focuses on an assessment of the FMI's practices against the standards set in the ECR and incident reporting guidelines. To facilitate these assessments, Bank staff request relevant documents, including cyber security frameworks, policies, and annual self-assessments. These documents form the basis of the initial offsite assessments.

100. At onsite meetings, BOC staff supplement the document review with targeted questions for management. These questions are an opportunity for Oversight staff to challenge the FMI. For example, overseers probe self-assessments and look for evidence that policies and frameworks have been consistently implemented. The BOC ensures that examinations cover the

entire set of expectations in the ECR. The BOC does not perform technical testing or verifications as part of onsite examinations.

101. The Bank's cycle for conducting cyber-CARs is every three years. During the last cycle, the following cyber-CARs were performed:

- 2022- Payments Canada (Lynx, ACSS) TMX Group (CDCS, CDSX) Interac (e-Transfer)
- 2023- Interac Inter-member network (IMN; review began in late 2023 following IMN's designation as a prominent payment system and ended in early 2024)

102. Generally, the Bank conducts CARs on each subject area every three years; however, the oversight framework is flexible, and the BOC can do off-cycle reviews if warranted, for example, through monitoring of industry trends or repeated risk events at an FMI. To date the BOC has conducted one thematic review for an FMI on third-party risk management, which has a cyber component.

103. As part of the CAR process, the BOC assesses whether designated FMIs meet the ECR. The review establishes any gaps in the FMIs' practices against the ECR. These gaps are used to develop potential risk scenarios. These scenarios are assessed against a likelihood and severity matrix to derive gap ratings, ranging from Tier 1 to Tier 4. Oversight staff propose remedial actions ("oversight expectations") to close gaps. A Bank governance committee—Oversight Risk Advisory Committee (ORAC)—provides a challenge to the staff recommendations on gap severity and proposed remedial actions.

104. As per the Bank's ECR, FMIs are expected to establish and maintain a comprehensive testing program as an integral part of their cyber resilience framework. The Bank is not involved in these tests, other than reviewing summaries of findings that are shared.

105. The ECR is used to assess third-party risk, and the BOC also applies the PFMIs, in particular, the assessment methodology for the oversight expectations applicable to critical service providers in assessing the FMI's third-party risk management practices.

106. The BOC does not share risk ratings, but key findings are shared with designated FMIs following CARs. Findings, or matters of concern, from all FMIs are reviewed annually by the Bank's ORAC to determine which become oversight expectations. These expectations (priorities) are formally communicated in writing to the senior management of the FMI and discussed with the Board of Directors.

107. Each oversight expectation communicated to an FMI includes an associated timeline for completion. The Bank follows-up semi-annually at Executive Meetings with senior management of the FMI and the BOC on the progress they've made in addressing each oversight expectation. Depending on the scenario, the BOC could request an audit or some form of professional acknowledgement that provides assurance that a recommendation has been remediated effectively.

However, typically the BOC seeks assurance directly from the FMI, in the form of updated documentation and information related to enhancements that have been implemented.

108. BOC has a robust and comprehensive approach to overseeing its FMIs. The ECR provides a holistic basis for overseeing and assessing FMIs, and the combination of offsite and onsite examinations allows the BOC to effectively monitor the FMIs' cyber capacities. There is a sufficient management challenge to the risk assessments conducted, and the processes to relay findings back to the FMI (and the subsequent follow up) ensures that FMIs can take the requisite steps to improve their defenses. During the FSAP assessment, the BOC provided a walkthrough of a recent CAR. The CAR methodology was robust, using the ECR as the basis; the documentation and evidence gathered from the FMI was detailed; the process to evaluate the evidence, analyze the root cause and the conclusions derived were mature; and the findings and report were clearly drafted and communicated to the FMI. The follow-up to the findings were timely and the BOC's oversight function demonstrates a strong process of continuous monitoring of its FMIs.

British Columbia (BCFSA)

109. The supervision of PRFIs is principles-based and focused on risk-based supervision (RBS). RBS requires sound judgment in identifying and assessing risks as well as determining, from a wide variety of supervisory and regulatory options available, the most appropriate method to ensure that the risks a PRFI faces are adequately managed. PRFI's and pension plan administrators are subject to BCFSA's Information Security Guideline, which is modelled after the NIST Cyber Security Framework, whilst Central 1[9] adheres to the ISO 27001 standard and is independently assessed on an annual basis as to how the information security management systems across all Central 1 operations meet the requirements set out in the ISO standard.

110. Offsite supervision is focused on the following information sources:

- Adoption of any new technology that may pose cyber risk to the regulated FI;
- Any major changes to systems that support critical business functions that may pose cyber risk to the regulated FI;
- Review of IT related internal audit reports to ensure any significant findings are addressed in a timely manner;
- Review of the enterprise-risk-management (ERM) dashboard and investigate material changes to the direction of the risk pertaining to cyber risk; and
- Review of Committee (i.e. IT Committee) meeting package and minutes to identify any issues or concern pertaining to cybersecurity and then follow up with regulated Financial Institution.

[9] Central 1 is a leading financial services partner, providing treasury, payments and digital solutions to nearly 300 FIs and their more than five-million members and customers across Canada, and is regulated by BCFSA.

111. In terms of onsite examinations, BCFSA follows the Information Technology Assessment Criteria and ensures the on-site review work covers all areas in the assessment criteria. In general, based on Information Technology Assessment Criteria, BCFSA prepares a list of interview questions to be used during the interview with key personnel from the regulated financial institution, including IT staff, management, and internal auditors. Through the interview, BCFSA verifies if there are appropriate processes and controls in place for the critical system, application, and data.

112. BCFSA has not conducted any credit union on-site cybersecurity examinations in the past 3 years, including Central 1. Furthermore, BCFSA has not performed a thematic cybersecurity review in the last 3 years.

113. In terms of proportionality, supervisors may apply different expectations based on the size and complexity of the regulated financial institutions. The expectations for systemic institutions are different compared to non-systemic institutions. For example, supervisors expect systemic institutions to have more robust business continuity plans and cyber incident response plans. The expectation (i.e. frequency and level of detail) on the management reports to the Board, pertaining to cybersecurity and operational risk, is also higher for systemic institutions.

114. To ensure consistency, an assessment criteria document is available for supervisors to ensure the same assessment criteria are used across different institutions. In terms of testing, per the BCFSA Information Security Guideline, regulated financial institutions are expected to establish and implement a testing process that validates the robustness and effectiveness of the security measures, and establish a process to receive, analyze, and respond to vulnerabilities and flaws disclosed to the organization. Regulated financial institutions may conduct penetration tests, vulnerability assessments, or table-top exercises that simulate a cyber-attack, depending on their size and complexity. While the supervisors are not involved in these tests, they review the reports and ensure critical/high importance findings are addressed in a timely manner.

115. In line with the BCFSA Supervisory Framework, supervisors, where appropriate, use the work of others to reduce the scope of the supervisory work. Supervisors may use the independent cybersecurity attestation or other assurance to help them assess the completeness and effectiveness of the controls. BCFSA accepts assurance reports from independent third parties as independent assurance. Furthermore, supervisors may use the cybersecurity self-assessment to help them assess the completeness and effectiveness of the controls. To validate the results, supervisors may conduct interviews with key IT personnel or compare them to other working papers to identify any inconsistencies or examine certain working papers if needed. Finally, supervisors may, where appropriate, rely on the work of internal audits, to reduce the scope of the supervisory work.

116. While there is no risk rating for individual findings, BCFSA prioritizes the findings by requirement (high priority), recommendation (medium priority), and observation (low priority), along with the due date by which institution must have a formal plan in place to address the findings. Supervisors follow up all findings that are either classified as requirements or recommendations.

117. Although the BCFSA has a well-structured RBS framework, there could be improvements to the cyber supervision processes. It is notable that the BCFSA has not conducted any onsite examinations in the last three years, including for Central 1, which is systemically important in British Columbia and beyond. However, this should be contextualized—the BCFSA is a relatively new authority, and in its first three years, it has largely prioritized its supervision on governance, strategy, and long-term viability of FIs. As a result, it has focused its cyber supervision mostly on continuous monitoring rather than onsite examinations. A further observation is that BCFSA does not have a specific cyber risk supervisor position and relies on one Subject Matter Expert that focusses on information security issues. As a result, there is a lack of resources dedicated to cyber supervision, which may be problematic given the large number of FIs it must supervise. Furthermore, whilst there is an Information Technology Assessment Criteria, aligned to the Information Security Guideline, it has not been mapped to the other Guidelines published by the BCFSA, that is, Outsourcing Guideline and Recovery Plan Guideline. The Assessment Criteria is a valuable guide for supervision, but it is not a supervisory manual, which should set out the processes for conducting proportionate offsite, onsite, and thematic reviews in a more detailed, lower-level and structured manner. Given the lack of cyber expertise amongst BCFSA's supervisors, a dedicated manual that maps all the cyber requirements from the different guidelines to it, would be particularly valuable for the more generalist supervisors.

Québec (AMF)

118. AMF's primary focus of cyber risk supervision is the governance of cyber risk and its integration to the global risk management framework for institutions. The supervision process is based on these guidelines: ICT guideline, Operational risk management guideline, Outsourcing risk management guideline, Business continuity guideline, Integrated risk management, and Governance guideline. However, it should be noted that there is no supervisory manual that sets out the processes for offsite, onsite, and thematic against all the cyber-specific requirements set out in the aforementioned Guidelines. Furthermore, the cyber-specific requirements in these Guidelines have not been mapped out yet.

119. AMF's off-site cyber risk supervision process is articulated around the following practices:

- Quarterly and ad-hoc meetings with structures in charge of managing operational, ICT, and cyber risks.
- Granular data that is required and analyzed minimally on a quarterly basis (e.g. operational incidents and loss structures). These analyses are used to challenge the institution.
- Regular meetings with the first, second, and third lines of defense to exchange/challenge their findings and action plans. Meetings are also organized with any relevant senior officers or teams. For example, the AMF organizes frequently meetings with the Chief Information Security Officer (CISO) or the chief compliance officer of the FI.

- The AMF requests a process for notification of material operational risk incidents. Every notification is analyzed and the appropriate structures within the companies demonstrate a timely resolution of the incident.
- Major initiatives like prioritization of critical activities, impact analysis, management of shadow banking, systems modernization, automation, ICT operations, and ICT risk management are also followed by the AMF. The AMF is currently asking its D-SIFI to develop indicators to link the deployment and operationalization of these initiatives to the reduction of operational risk.
- The quantitative analysis is added to these efforts to have a complete picture of the exposures of the companies in the AMF's jurisdiction.

120. The AMF's risk profiles of its regulated entities are updated minimally annually with these mechanisms and the output of on-site supervisions. More specifically, the main cyber risk areas supervised by the AMF are aligned with the six domains defined by the 2024 NIST (CSF) framework.

121. The AMF's onsite examinations are based on the Financial Institutions Supervisory Framework and the Guideline on Information and Communications Technology Risk Management. The scope of the AMF's examinations is based on the financial institution's risk assessment and the proportionality principle and covers the following subjects:

- Types of ICT risks (Taxonomy)
- ICT governance
- ICT risk management
- Organizational framework
- Cybersecurity policies
- Supply chain risk management
- Asset management
- Risks assessments
- Identity and access management
- Security Training and awareness
- Data security measures
- Platform security

- Technology infrastructure resilience
- Monitoring
- Security event monitoring
- Incident management and reporting
- Resilience, business continuity and disaster recovery
- Network security
- Vulnerability and patch management
- Intrusion testing
- Independent conducted cybersecurity posture maturity assessments
- ICT and security architectures

122. When performing examinations, the AMF will ask for all relevant documentation pertaining to the scope as determined by the proportionality principle. The AMF will meet and interview with relevant personnel including high level executives such as the VP of IT, the CISO, the VP of audit, and the VP of Compliance. The AMF will examine Board meeting minutes and submit reports on cybersecurity and risks, including those to the audit and risk committees. The AMF also receives regular reports from the second line of defense (Integrated Risk Management), which may include cyber risks assessments. In the last 3 years, the AMF has performed 10 on-site cybersecurity examinations, but no thematic reviews on cybersecurity.

123. The AMF expects FIs to obtain independently conducted cybersecurity maturity assessments and penetration tests and/or red team tests. The AMF does not impose any framework for these assessments, and the AMF is not involved in their execution. The AMF recommends internally conducted maturity assessments, intrusion testing and risk analysis according to their cybersecurity maturity posture, ICT cybersecurity practices and risk management practices. For regulated entities with a high-risk profile in the securities sector, the AMF requires vulnerability and penetration testing to be performed and the results to be provided on a quarterly basis. The AMF follows up on observations and further investigates with the information security office when necessary.

124. The AMF relies on independently conducted assessments of the cybersecurity maturity, intrusion tests and security controls appropriateness and efficacy. These assessments are an important part of the AMF's examinations and are used to evaluate the comprehensiveness and the maturity of the financial institutions' cybersecurity controls and as a comparison to the cybersecurity posture of the FI's peers.

125. The AMF relies on the FI's self-assessments to a lesser degree, mostly as a measurement of progress of security initiatives or actions plans. The AMF validates their results with the independently performed assessments or with third line of defense assessments on a case-by-case basis.

126. The AMF communicates the findings and the severity rating of the recommendations of the examination to the concerned FI. The AMF follows up on all recommendations from its examinations. FIs are expected to respond within 30 to 45 days after receipt of the examination report and its recommendations. The AMF relies on the institution's third line of defense to provide assurances on the appropriateness and on effectiveness of the implementation of the cybersecurity measures outlined in the recommendations on a case-by-case basis, as well as independent cybersecurity auditors.

127. The AMF has a sound cyber supervisory framework, which includes onsite and offsite examinations. However, there are a significant number of guidelines that FIs must adhere to, and these should be analyzed and mapped to cyber-specific requirements, and thereafter integrated into the supervisory assessment processes, documented in a dedicated cyber supervisory manual.

Canadian Securities Administrators

128. The securities regulators monitor and assess compliance of clearing agencies with the systems review requirements described in NI 24-102. More precisely, the periodic reviews must include an assessment of how clearing agencies are compliant with the regulatory requirements. To this end regulated entities must conduct an annual self-assessment, further to which the relevant securities regulator conducts its own annual risk assessment.

129. As part of their offsite cyber risk supervision process for clearing agencies, the relevant provincial securities regulators mandate the provision of quarterly information on cyber security events identified, threats and vulnerabilities identified, penetration tests performed, and the training and awareness exercises conducted (Quarterly Cybersecurity Report). In addition, where a security incident has occurred, the relevant provincial securities regulators require a full report on both the incident and steps to remediate any issues identified because of the incident and monitor action to remediate issues identified.

130. The securities regulators, jointly with the Bank of Canada, participate in a quarterly call with the clearing agencies to review the results of the quarterly cyber-security report and operational risk events. The relevant securities regulators also track the clearing agencies' remediation of their self-identified exploitable vulnerabilities.

131. The focus areas of the on-site cybersecurity examinations conducted by the securities regulators are based on the results of the annual risk assessment mentioned above and target the specific risks identified. Previous inspections of clearing agencies focused on the following topics:

- The organizational structure, including the roles and responsibility of the information security department, senior management and the Board;
- IT security surrounding APT (Advanced Persistent Threats) attacks;
- The results of disaster recovery tests;
- Internal audit IT risk assessment and monitoring work;
- Processes and the procedures pertaining to IT;
- Clearing agency's policies and procedures relating to security, including the oversight of security measures of third-party service providers; and
- Reports and other records provided by internal audit, external auditors, vulnerability and penetration testers, and other third parties.

132. It should be noted that the securities regulators have not performed an on-site cybersecurity examination of clearing agencies in the last 3 years for various reasons, including CDCC implementation of a new risk system in 2019 and CDS modernization of its clearing and settlement system, which began in 2018 and is still ongoing. The securities regulators' most recent IT related examinations were completed in 2015 and in 2018.

133. Through the CSA, the securities regulators coordinate and harmonize the regulation of clearing agencies. This includes harmonizing the terms and conditions of clearing agencies, allowing for similar reporting requirements and coordinated oversight. Similar harmonization efforts also take place for clearing agencies subject to joint provincial-federal oversight.

134. The securities regulators use a formal rating system to assess the risk profile, ensuring uniformity across clearing agencies. Annually, the risk rating of each clearing agency is benchmarked against each other and previous years ratings to identify changes and trends in risk profiles.

135. For clearing agencies, the relevant securities regulators rely on the annual system reviews of the clearing agencies performed by external auditors, as required under NI 24-102. Clearing agencies must perform vulnerability and penetration testing and provide the results on a quarterly basis. The relevant securities regulators follow up on observations with the clearing agencies, as required, based on the outcome of testing and review of reports provided by the clearing agencies and may further investigate with the information security office when necessary. When applicable, the relevant securities regulators and the BOC will, to the extent possible, coordinate follow-up actions. Furthermore, the oversight programs and expectations of the securities regulators include self-assessments, the results of which are evaluated and tested by the securities regulators.

136. Within 30 days following receipt of the final oversight review report, the clearing agency must submit an action plan that includes timelines for addressing all the findings and/or a description of the corrective actions that it has already taken. If necessary, the clearing agency must implement compensating controls until the finding is appropriately resolved. In some circumstances, the action plan must be prepared by a representative of the clearing agency's senior management, then approved by the board of directors or a board committee. Depending on the significance of the findings and/or the response provided, a shorter timeline or corrective actions in addition to or different from those presented in the action plan may be required.

137. The securities regulators periodically follow up on the clearing agency's progress in implementing its action plan to resolve the findings set out in the oversight review report. This follow-up is part of an ongoing process and is performed to ensure that actions taken based on the findings are coherent and adequate and are implemented according to the timelines specified in the action plan. Any changes that affect the corrective actions or timelines must be communicated to the securities regulators.

138. Overall, the oversight framework for these regulated clearing agencies is robust and the cooperation between CSA, securities regulators and BOC is well-defined, with clear processes and information sharing. Each of the securities regulator conducts its own annual risk assessment, and there is sufficient collaboration, coordination, and communication between all the relevant authorities. The joint approach allows for cross-fertilization of views and analysis. Notwithstanding this, the authorities acknowledged that the process for joint oversight is continuously evolving and improving. Within this context, it is essential that the CSA and respective regulators conduct an onsite examination of the CSD and CCP with regard to cyber resilience. Furthermore, as there are regulatory requirements from two counterparts (i.e. BOC and securities regulators), it would be useful and more efficient to map the regulatory requirements to a standardized oversight methodology that could help guide the authorities in conducting joint oversight in a more efficient and resourceful manner. Both sets of authorities have indicated that they are undertaking this work at the moment and there is intent to further integrate their oversight processes and methodologies, especially as the BOC and AMF are due to conduct a joint Core Assurance Review.

Recommendations

- BCFSA and AMF should review and map all of their Guidelines to identify the cyber and technology-specific requirements and thereafter develop a supervisory manual that includes these requirements and sets out the process for onsite, offsite, and thematic reviews to supervise them, in line with the RBS framework.

- BCFSA should conduct onsite examinations for cyber resilience on its most systemic PRFIs, including Central 1[10].
- BCFSA should consider increasing its staffing and/or expertise in cyber supervision.
- CSA members and BOC should conduct an onsite examination related to cyber resilience of its regulated entities.

B. Incident Reporting Arrangements

139. OSFI, BOC, BCFSA, AMF and CSA all have comprehensive cyber incident reporting regimes in place. All authorities have clear definitions for cyber incidents, severity ratings/thresholds, timelines for reporting, and clear procedures for reporting. Their approach places them ahead of other jurisdictions, where developing and operationalizing an incident reporting regime remains a key challenge. Financial entities must report cyber incidents to their respective financial authorities. However, the incident reporting regimes do not consistently require third-party providers to report incidents, and it was noted that if there is an incident at a provider, FIs may not be able to report such incidents due to confidentiality and legal constraints.

140. The incident reporting regime is mature, and the authorities receive incident notifications in an efficient manner. The authorities review the notifications and are able to judge the severity of each incident. OSFI's TRD receives as many as 2000 incident notifications per year and has a robust process to review the incidents, invoke incident response protocols if required, analyze annually the incidents on an aggregate level, and disseminate an analysis of the incidents to FRFIs.

141. Notwithstanding this, the authorities could improve the sharing of relevant incident information with each other when appropriate and if feasible, as well improving convergence. For example, BCFSA and AMF are not informed of relevant incidents in British Columbia and Québec by OSFI. Even though such incidents relate to OSFI-supervised entities, there may be utility in both authorities sharing relevant incident information between each other. Currently, it has been noted that confidentiality restrictions present an obstacle to sharing such incident information; however, as incidents could easily spill over into the provinces, sharing relevant incident information would allow each regulator to prevent potential financial stability risks from materializing. Furthermore, entities that are overseen by multiple authorities indicated that whilst initial notification of an incident to its regulators is standardized and efficient, follow-up incident reporting can be cumbersome due to different requirements and templates.

Recommendations

- Given the large number of federal and provincial authorities in Canada, the authorities could benefit from reviewing the work of the FSB's Cyber Incident Reporting working group which is

[10] Central 1 is a leading financial services partner, providing treasury, payments and digital solutions to nearly 300 FIs and their more than five-million members and customers across Canada, and is regulated by BCFSA.

developing a standard for incident reporting to achieve global convergence and facilitating cross-authority information sharing. It would be advisable for Canadian authorities to collectively review their existing incident reporting regimes, update them in line with the FSB's framework Format for Incident Reporting Exchange (FIRE) and align them as much as possible, and consider mechanisms for cross-authority information sharing of relevant incidents, when appropriate and if legally feasible. Furthermore, authorities should consider how to integrate third-party providers into the reporting processes.

- The federal authorities should undertake a legal review and take the necessary steps to facilitate the sharing of relevant incident information between federal and provincial regulators.

C. Supervisory Resources

Office of the Superintendent of Financial Institutions

142. OSFI takes a risk-based approach in ensuring that there is adequate capacity to supervise technology and cyber risk at FRFIs. Every year, supervisory planning is done jointly with the Supervision Sector to ensure that there are adequate resources based on risks. Currently, TRD has 29 full-time employees. OSFI has also developed tools to train supervisors on how to assess technology and cyber risks for smaller FRFIs. A dedicated team is accountable for incident management and response within TRD to ensure it can investigate and respond with urgency. This incident response team has grown from one resource to five in the past two years because of the need to analyze and respond to an increasing number of incident reports. Other tools are being looked at to reduce manual processes and increase automation such as the end-to-end automation of the incident management processes. However, there has been slow progress in this regard because of a lack of dedicated IT resources (to make this a priority) and funding.

143. Recognizing the importance of emerging cyber and technology risk, the CATTIC team was established in 2022 to identify and monitor macro cyber and technology threats and risks within the financial sector. Their threat risk assessments contribute to determining the prioritization and response of OSFI's top external risks in accordance with its risk appetite statement. Currently there are 3 full-time employees in CATTIC.

144. The collective functions inside OSFI allow it to identify both traditional/commercial-level cyber risks as well as sophisticated/classified cyber threats that may affect the safety and soundness of the financial sector. OSFI can apply this threat information for the supervision of individual institutions and contribute to the sector overall. OSFI's legislative authorities allow it to take a range of supervisory actions. OSFI also works with CCCS and other partners to facilitate threat information sharing with the institutions within OSFI's oversight.

145. In 2023, OSFI established a NSS to support its mandate to consider if FRFIs have adequate policies and procedures to address threats and risks related to integrity and security, including foreign interference. The NSS will examine integrity and security risks,

including foreign interference, that could affect FIs. It will also provide national security assessments, advice, and intelligence co-ordination within OSFI.

Bank of Canada

146. The BOC's approach to strengthening cyber risk supervisory capacity in FMI oversight is to leverage the expertise of subject matter experts. The FMI oversight team includes two full-time cyber specialists. Additionally, Oversight has an agreement with the Bank's Information Technology Services department to get additional technical support as required.

FINANCIAL SECTOR RESILIENCE

A. Information Sharing Arrangements

147. Although the information and intelligence sharing ecosystem in Canada is mature, there is room for improvement. There are several external stakeholders that provide the financial sector with threat information and intelligence.

Office of the Superintendent of Financial Institutions

148. OSFI shares information, without disclosing confidential information with FRFIs through various means. These include:

- Issuing technology and cyber bulletins across the sector on any themes and trends that OSFI is seeing around technology and cyber risks and threats. In the past 24 months, OSFI has issued several bulletins (e.g. MOVEiT transfer vulnerability, HTTP/2 Rapid Reset vulnerability, ransomware and API security, amongst others).
- Issuing an annual report on themes and trends noted around incident reporting. The report aims to share themes, trends, and root causes of technology and cyber security incidents reported to OSFI.
- Sharing, every quarter, incident trends, insights, and themes when meeting with the large banks and insurance companies to discuss technology and cyber risks.
- Participating in CFACT, a new initiative to identify and share key risks, vulnerabilities, and opportunities in the financial sector. Membership includes all FISC agencies along with the CCCS and the Financial Transactions and Reports Analysis Centre (FINTRAC).
- OSFI also meets quarterly with the US Treasury to share information on cyber topics together with the DoF, BOC, and Payments Canada.

Bank of Canada

149. The BOC chairs the CFRG, which acts as the Canadian critical financial sector's primary forum for sharing information and coordinating a response related to operational incidents (including cyber) between the government and private sectors. Information sharing is on a voluntary basis.

150. The BOC is also a member of the Financial Services Information Sharing & Analysis Centre (FS-ISAC), which was originally formed in the United States but has since expanded to become a worldwide organization. FS-ISAC Canada has been active since the early 2010s and involves many major players from across the country's finance sector. The group provides intelligence to its members.

Canadian Centre for Cyber Security

151. There are arrangements in place within the finance sector that CCCS participates in for cyber information and intelligence sharing.

152. CCCS collaborates with FIs and communities of interest to share threat intelligence. CCCS is a member of high-level trust groups within the Canadian finance sector, discussing current intelligence and incidents with partners. CCCS has developed capabilities for sharing IOCs and receiving intelligence reports from partners, offering additional insights into the financial landscape.

153. The Canadian Cyber Threat Exchange (CCTX) is a Canadian organization whose goal is to provide access to timely, relevant and actionable cyber threat information. CCTX is an aggregator that provides the CCCS with wide distribution to Canadian critical infrastructure organizations. CCTX Board members include representatives from large Canadian private-sector organizations, many in finance, energy, telecommunications, and transportation sectors. CCCS participates in the weekly threat calls, where members share cyber threat information and trends. Moreover, CCTX Data Exchange is used to analyze and share cyber threat information, while their portal provides members with a forum to exchange information about best practices and techniques. Although the CCTX appears to be a technical mechanism for sharing intelligence, it is unclear what proportion of the financial sector, both federal and provincial, are involved in it.

154. Within the private sector, there is a limited number of large banks that have access to threat intelligence from the CSE, however, access to this level of intelligence is not available to other large systemically important FIs. There is also a CISO network, Canadian CISO Collaboration (C3) which is an offshoot of FS-ISAC Canada and brings together private sector CISOs to share information with each other informally. However, there is no automated platform that facilitates easy sharing of strategic, operational and tactical information.

British Columbia (BCFSA)

155. BCFSA is not part of a cyber information or intelligence sharing arrangement at the provincial level, although it does participate in the CCCS Cyber Threat briefings. In terms of the market participants, there is no information and intelligence sharing network at the provincial level.

156. There are general information sharing arrangements in place with other regulators through Credit Union Prudential Supervisors Association (CUPSA). There are, however, no information sharing arrangements with the federal regulator, that is OSFI.

Québec (AMF)

157. Many members of the financial sector are members of FS-ISAC, but the AMF is not on this platform. The AMF and many organizations of the Canadian financial sector work with the CCCS, a central resource where information on cyber threat intelligence and best practices are shared.

158. Overall, there are a number of key stakeholders in the Canadian financial ecosystem that drive the sharing of information and intelligence. However, there are gaps in the maturity of information and intelligence sharing between the federal and provincial sectors. Whilst entities benefit from the intelligence (e.g. strategic, operational and tactical) provided by CCCS, OSFI, and BOC, not all provincial entities have access to that level of information and intelligence. Second, whilst FS-ISAC is an efficient source of commercial threat intelligence, it is not a platform that is designed to build trust amongst smaller networks of entities that can share actionable intelligence with each other ex-ante. Finally, there does not appear to be any threat intelligence sharing between the federal and provincial entities. And information and intelligence sharing initiatives appear to be ad-hoc, not accessible to all, and unstructured or not formalized.

159. 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. By exchanging cyber intelligence within sharing communities, 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.

160. The Canadian financial sector would benefit greatly if federal and provincial entities participate in industry-wide information and intelligence sharing networks, and if there were more structured mechanisms of information and intelligence sharing between the federal and provincial communities across Canada.

161. Discussions with the private sector highlighted the desire for effective information and intelligence sharing amongst the community, with more entities being able to access such intelligence in a structured manner, and for such information to be available via automated

platforms and through in-person networks. However, concerns were also raised that such information sharing is limited due to legal constraints around information sharing, with a view that sharing cyber information and intelligence is wrongly considered as contravening data privacy. Furthermore, concerns were raised about legal liability issues around information sharing, which may lead FIs to being reluctant to share freely. It would be useful for a legal review to be conducted by authorities on confidentiality issues and information sharing, and where appropriate, legal exemptions to be given to facilitate information and intelligence sharing under the pretext of financial stability and national security. Removing potential barriers could significantly ease the free flow of ex-ante information and intelligence, which could enhance the overall protection of the financial sector.

Recommendations

- Federal and provincial authorities should work with their respective financial sectors to develop and operationalize cyber information and intelligence sharing networks. Authorities would benefit from taking a structured approach to develop these networks, engaging closely with the industry, to design the model and their operations. This should include[11]:
    - Drafting 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; and
    - Setting out the principles for sharing and analyzing information.
- As information and intelligence sharing networks are established at federal and provincial level, authorities should consider how to improve the sharing of such information and intelligence with each other in a systematic and structured manner, potentially using the Sector Network as a basis for coordination and establishing a network of networks.
- Federal and provincial authorities should conduct a legal review on information and intelligence sharing, to facilitate the sharing of such information without legal barriers (if feasible and permissible). Furthermore, it would be useful to promote information and intelligence sharing amongst FIs without fear of legal liability issues being used against them.

[11] In some jurisdictions, such a network is also established through a Financial Sector Computer Emergency Response Team (FINCERT), which Canadian authorities and CCCS could also explore.

B. Cyber Testing and Exercises

Testing

162. OSFI has developed and published its Intelligence Led Cyber Resilience Testing (I-CRT) Framework in April 2024. The current scope of the I-CRT framework applies to all Systemically Important Banks (SIBs) and Internationally Active Insurance Groups (IAIGs) which OSFI will cover on a 3-year cycle.

163. The Threat-led Penetration Testing (TLPT) framework is largely modelled on the UK's CBEST framework and the ECB's Threat Intelligence Based Ethical Red-teaming (TIBER-EU) framework and is in line with the G7 Fundamental Elements for TLPT.

164. TLPT or 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 (e.g., its people, processes, and technologies). It helps an entity to assess its protection, detection, and response capabilities. Thus far, OSFI has overseen two-three tests on FIs, in line with its I-CRT.

165. While the I-CRT is a well drafted framework and a useful tool for the supervisors to assess the cybersecurity of FIs, it is still in its infancy. Therefore, it will be important for OSFI to monitor its implementation, to assess whether further changes should be made to the process. Further, implementing such frameworks is extremely resource-intensive and requires supervisors with the right level of skills and expertise. Therefore, it is essential that as the framework is further operationalized, OSFI monitors its resource and skills requirements.

166. In line with other similar international frameworks, the I-CRT requires tests to be conducted on live production systems, which increases the potential risk associated with such tests. As a result, it is essential that such complex and potentially risky tests are conducted by the most competent and qualified threat intelligence and red-team test providers. In the case of the UK, a CBEST test can only be performed by providers accredited by the Council of Registered Ethical Security Testers (CREST), whilst in the TIBER-EU framework, there are clearly set out criteria and conditions for such providers. The purpose of accreditation or setting the criteria and conditions for providers was to ensure that such critical tests can only be performed by appropriate providers and personnel, thereby reducing the risk. The I-CRT framework currently does not mandate accreditation nor set out the criteria and conditions for providers. OSFI should consider incorporating such criteria and conditions into the framework.

167. TLPT tests are significantly expensive, and experiences in other jurisdictions have shown that the threat intelligence phase can be improved and made more cost effective. One way of doing is to introduce the concept of a GTL report to the framework. A GTL report elaborates on the specific threat landscape of the Canadian financial system, taking into consideration the geopolitical and criminal threats unique to the jurisdiction. The report would

consider key financial market participants and their critical functions, including (wholesale and retail) banks, broker dealers, financial market infrastructures, financial market utilities, other critical third parties, the different threat actors (including their tactics, techniques, and procedures) targeting these entities, and the common vulnerabilities. This GTL could be used by the different FIs undertaking the TLPT, to help inform the specific threat assessment for them, and may reduce the overall costs of the test, as those undertaking the test would complement the GTL with a narrower targeted threat intelligence report.

168. The GTL could also be used by authorities to better understand the threat landscape and foresee attack patterns and work with the FIs to better prepare for potential attacks through scenario development, building playbooks and exercising. Canada is well placed to develop a GTL, with highly mature agencies such as CSE, CCCS, BOC, RCMP (amongst others) having threat intelligence related to Canada and being effective stakeholders in developing it. In the first instance, the CCCS is perhaps best placed to develop such a GTL.

169. OSFI's TRD has indicated that a future deliverable is the development of an I-CRT Lite Framework, and to this end, the future framework would benefit with the inclusion of other types of more economical tests, such as Purple and Gold team testing. These are highly useful tests, and their cost-effectiveness would enable a more proportionate implementation amongst a broader and larger set of FIs, whilst also providing OSFI with sound assurance on the FIs' cybersecurity posture.

170. BOC, BCFSA, and AMF do not have a dedicated TLPT testing framework in place. Although these tests should be applied to mature and systemically important entities, other authorities (federal and provincial) should consider its use for its systemically important entities (e.g. FMIs).

Recommendations

- OSFI should monitor the implementation of the I-CRT Framework and ensure that it has the right level of resources and expertise for its successful deployment.
- OSFI should include, in the I-CRT Framework, clear criteria and conditions for threat intelligence and red-team testing providers, thereby ensuring only appropriately qualified providers can conduct an I-CRT test.
- CCCS should consider developing a GTL (in close collaboration with other relevant agencies, such as the RCMP and CSE).
- OSFI should consider updating its framework, in the longer term, with the integration of a GTL component, purple and gold team testing, and use the potential GTL for other purposes such as developing playbooks, scenarios and conducting exercising.
- The BOC and other provincial regulators should consider applying the I-CRT for their own systemically important FIs.

Exercising

171. 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.

Office of the Superintendent of Financial Institutions

172. OSFI participates in cyber exercises conducted by the CFRG and G7 Cyber Expert Group (CEG). Other than this, OSFI conducted one exercise that included two banks in 2020 and aims to conduct a further exercise as part of its 3-year plan. However, such exercises have been limited to date.

Bank of Canada

173. Under the BOC's leadership, CFRG held two industry-wide exercises to test the CFRG Crisis Coordination Playbook. Exercise participants included CFRG's executive Steering Committee members. The exercise led to several Playbook updates, including documenting key processes related to public-facing communications and coordination.

174. In 2024, CFRG and the Canadian Securities Telecommunications Advisory Committee (CSTAC) partnered on the first cross-sectoral exercise between the financial and telecommunications sectors. Exercise participants included the executive Steering Committee members of both CFRG and CSTAC (over 40 organizations). The CFRG and CSTAC are in the process of actioning the exercise findings, which includes formalizing cross-sector crisis coordination processes during incidents.

Canada Deposit Insurance Corporation

175. CDIC conducted a tabletop exercise with the CDIC Board of Directors in April 2022. The objective was to explore CDIC's role and the potential use of its toolkit—within the broader financial safety net framework—in the event a D-SIB was impacted by a cyber-attack and its depositors were unable to access their deposits for a prolonged undefined period as a result.

176. The exercise facilitated a conversation on the role of CDIC as resolution authority and deposit insurer in an event where a D-SIB's critical services are interrupted by an operational event and confidence in the system is jeopardized. It resulted in the exploration of whether CDIC, in collaboration with the financial sector agencies, should have a role in facilitating access to deposits in case of a member institution experiencing operational challenge, for example, as a result

of a cyber-attack. Overall, the simulation was a valuable and proactive exercise that contributed to the CDIC's overall preparedness.

177. CDIC has also participated in exercises through the CFRG. However, while CDIC has conducted exercises with FIs in the context of its bail-in powers, it has not conducted an exercise with FIs as participants against the backdrop of a cyber event.

British Columbia and Québec

178. The BCFSA has not conducted any cyber exercises with its FIs, nor was it involved in the BOC's exercises as it is not a member of the CFRG. The AMF has also not conducted any exercises on its sector, although it was involved in the CFRG exercises.

179. Whilst the exercises conducted have been positive, it would be recommended that such exercises are conducted more frequently. Such exercises are crucial to build resilience and enhance crisis preparedness, and the number of tests conducted to date has been very limited, and also, limited in terms of the financial sector participants that have been involved (e.g. no insurance companies, no Central 1, etc.).

Canadian Securities Administrators

180. The securities regulators formed the Market Disruption and Cybersecurity Coordination Group (MDCCG) in 2017 for the purpose of improving communication and information sharing between participants and regulators in securities markets in the event of a large-scale market disruption, including a large-scale cybersecurity incident. The group was comprised of representatives from the CSA Market Structure and Exchange Oversight Committee, amongst others. In developing a more formal CSA coordination process to manage a market disruption including one that stems from a cybersecurity incident, the MDCCG collaborated with other regulatory authorities, including Canadian Investment Regulatory Organization (CIRO), OSFI, and the Bank of Canada.

181. The MDCCG developed the CSA Market Disruption Coordination Plan (the CSA Plan) in 2018. Since then, staff from the various CSA oversight committees carry out periodic testing and make updates to the CSA Plan. In 2021 and 2023, oversight staff across the securities regulators participated in the CIRO biennial industry Business Continuity Plan (BCP) test. This included a market disruption simulation component which allowed for the testing of the CSA Plan. The most recent CIRO BCP test was conducted in December 2023, which was based on a scenario of a systems issue affecting TSX (the largest Canadian stock exchange, which shares a parent company with CDS and CDCC) that led to trade breaks the next day and spawned rumors of a coordinated cyber-attack on Canadian marketplaces and clearing agencies.

Third-party Providers and Exercises

182. Third-party providers play a critical role within the Canadian financial sector, as well as other sectors. Even though they fall outside the legal and regulatory perimeter, they can still be

involved as participants in such cyber exercises. This would potentially help in fostering relationships between the authorities, the broader financial sector, and the critical third-party providers; integrate such providers in the sector-wide incident management processes; and facilitate potential information sharing between all parties, thereby leading to stronger cyber resilience across the ecosystem.

Recommendations

- DoF, BOC, OSFI, BCFSA, and AMF should conduct regular (e.g. annual) cyber simulation exercises with other authorities, sectors (e.g. telco) and a broader selection of financial entities in their federal and provincial sectors (e.g., banks, FMIs, insurance companies, etc.), including third-party providers.

- The proposed financial sector network, which brings together different federal and provincial authorities across Canada, should work together in sharing their experiences of exercises, scenarios, approaches, results, so they can effectively collaborate and take a more structured and standardized approach to cyber exercising. In doing this, each federal and provincial authority will improve its public-private coordination within its respective sector, build cyber awareness across the entire Canadian financial system, and improve its respective sectoral cyber incident response framework.

C. Systemic Response and Recovery

Office of the Superintendent of Financial Institutions

183. OSFI chairs the FISC. Although this forum does not have a specific role on cyber risk matters, it is flexible by design and can be used to coordinate on cyber risk issues in the financial sector as needed. Coordination mechanisms for cyber risk in this forum are not outlined in formal agreements, however, there are more formal approaches to agency communications methods. Through the FISC, OSFI has put in place sector-wide crisis communication protocols for its regulated entities.

184. OSFI has contingency plans and crisis communication protocols that would be used in the event of a largescale cyber-attack. This includes the OSFI Technology and Cyber Incident Response Protocol, which is a well drafted plan on how to manage a cyber incident at an FRFI. The TRD has a strong team that continuously monitors incidents (e.g. using tools such as Down Detector), equipping it with the right capabilities to invoke the incident management protocols.

185. As part of the Government of Canada, OSFI follows the CCCS's guidance which includes playbooks. Moreover, OSFI is in the process of developing updated playbooks to respond to various types of incidents (e.g., Ransomware).

Bank of Canada

186. As per the BOC's Incident Reporting Guidelines, designated FMIs must inform the Bank promptly of significant cyber events. The FMIs maintain contact lists of key Bank personnel and vice versa. If Bank oversight staff receive notice of a significant incident, they report it to senior management immediately. There is also a notification to other internal stakeholders for awareness, including IT Services and Financial Stability.

187. Depending on the nature of the incident, it could be escalated further, invoking formal crisis management protocols. For incidents that could have a material impact on the soundness of an FMI, the Idiosyncratic Crisis Management Advisory Committee (ICMAC) would be invoked. This would ensure a comprehensive response to the incident, which could include lending to the FMI, or declaring the FMI non-viable and invoking the Bank's resolution authority. The ICMAC would also advise on any related public communications.

188. Additionally, a cyber event that could have a financial system-wide impact would trigger the CFRG. This group would co-ordinate responses and advise on public communications. The CFRG acts as the Canadian critical financial sector's primary forum for sharing information and coordinating a response related to operational incidents (including cyber) between the government and parts of the private sectors. In this regard, the CFRG has developed a Crisis Coordination Playbook which is intended to cover potential or actual systemic operational incidents (including cyber incidents). However, it is important to note that the CFRG brings together the different entities in a crisis, to share information, but is not a decision-making body. Its mandate explicitly states: "CFRG is not a decision-making body, although it can influence decision-making bodies to fulfil its mandate".

Department of Finance

189. The DoF maintains a cyber contingency plan in case there is a largescale cyber-attack on the financial sector. Finance is also part of the FISC processes, through which the DoF has in place crisis communication protocols. Finally, the DoF has developed an Interagency Cyber Preparedness Playbook which is intended to outline the protocols and agreements in place in the financial sector that serve to establish how FIs and financial sector agencies would share information and liaise with one another in the event of a cyber incident affecting the financial sector. The playbook aims to present an overall picture of how cyber incidents are managed in the financial sector; who are the key players; and what are the main reference documents.

British Columbia (BCFSA)

190. If there is a largescale cyber-attack that materially impacts a regulated financial institution's operation, BCFSA may activate its Crisis Communication Plan. However, there is no playbook for different cyber scenarios that the PRFIs might encounter, and the plan has not been tested.

Québec (AMF)

191. At the AMF, each business sector has its own business continuity plan ("BCP"), which were last updated in 2022. Since January 2024, the Integrated Risk Management and Performance function is responsible for centralizing and updating the plans in collaboration with the business lines. Each business continuity plan owner ensures that their business continuity plan adequately reflects the sector's business continuity capability. All the business continuity plan updates are part of the implementation of the AMF's operational resilience program. The AMF's response structure defines the necessary roles, authority and skills required to manage a largescale cyber-attack.

192. The corporate business continuity policy is approved by the CEO and describes the main principles to be implemented, in particular by ensuring that the various BCPs are linked to each other and with the organization's other emergency plans (ex. Crisis management plan). This policy is available to all employees on the AMF's corporate intranet portal.

193. The AMF has 13 playbooks based on the most common cyber threat to facilitate its incident management to many attack scenarios or cyber events that could occur. The playbooks include response, notably to phishing, malware, data leak, intrusion, and Distributed Denial of Service (DDoS) scenarios. However, this BCP is largely internal and there is no sector-wide crisis management plan and crisis coordination playbook, which can be invoked when an incident occurs within the financial sector and could potentially impact the broader financial system in Québec.

194. Efficient and effective response to and recovery from a cyber incident by authorities in the financial ecosystem are essential to limit any related financial stability risks. Such risks could arise, for example, from interconnected IT systems between multiple financial entities or between financial entities and third-party service providers, from loss of confidence in a major financial entity or group of financial entities, or from impacts on capital arising from losses due to the incident. Consequently, enhancing cyber incident response and recovery (CIRR) is an important focus for authorities and such authorities have an important role to play in responding to cyber incidents that present potential risks to financial stability.

195. Whilst there are bodies and structures in the federal agencies to manage a systemic incident (e.g. FISC, CFRG and SAC), there is no overall specifically cyber dedicated decision-making structure in case of a systemic cyber incident that could impact the financial sector. Such a body can be formally invoked in the specific case of a cyber incident that could have systemic implications and spillovers into the different types of FIs and FMIs, and into other sectors. In such circumstances, it is essential that there is an "Authority's Response Framework", that allows all the relevant stakeholders to coordinate and communicate, with clear decision coordination and clarity on actions to be taken, when the threshold for systemic cyber risk is breached. Although the nature of decisions will differ depending on the nature of the incident, some scenarios may require invoking emergency lending, or disconnecting FIs from the FMI network, or making public statements to the media, or interacting with international regulators at the highest level.

196. It should be noted that both the SAC and FISC have the flexibility within their mandates to address systemic cyber incidents. Given that FISC is led by OSFI, it is well-positioned to initiate discussions on cyber events impacting FIs. If an issue arises that extends beyond FISC's FI focus, the SAC (Chaired by the Deputy Minister of Finance) can take the lead in facilitating such discussions and make decisions and/or recommendations for the broader financial sector, if needed, to the Minister of Finance. The membership of both committees includes principal decision-makers, such as deputy heads, and can invite additional deputy heads or their delegates as needed. This ensures access to the necessary expertise and enables rapid, informed decision-making when required. Although the structures exist, the authorities could benefit from formalizing the overall decision coordination within these structures specifically for systemic cyber incidents, with clearly defined criteria and threshold of systemic cyber incidents, and a clear playbook of cyber scenarios, that are regularly tested.

Recommendations

- The federal authorities (e.g. Finance Canada, BOC, OSFI and CDIC) should consider leveraging existing structures (e.g. FISC, CFRG, SAC, etc.) to put in place a process to manage a systemic cyber incident, with decision coordination, clearly defined criteria and threshold of systemic cyber incidents, and with a clear playbook of cyber scenarios, that are regularly tested.

- The AMF and BCFSA should develop and document a sector-wide crisis management and coordination plan, as well as playbooks for different extreme but plausible cyber scenarios.

D. Systemic Analysis and Concentration Risk

197. OSFI, BOC, BCFSA and AMF do not develop cyber maps of their respective financial sectors; they have not identified and documented transmission channels through which cyber risks can affect financial stability; they have not identified and documented cybersecurity risk contagion scenarios; and they have not included cyber risk in their stress testing programs. It would be useful to analyze and document the different transmission channels that could trigger financial instability via cyber-attacks, including the range of different contagion scenarios that could cause disruption to the financial sector. This would enable the authorities to understand the potential impact on the system and develop mitigation strategies or actions that will be taken by them to manage the crisis.

198. Not all the authorities collect relevant information and data, such as identifying vendors and service providers of IT systems used by financial entities for their core business and identifying the status of major external systems (e.g., connections to other systems, participating entities, and providers' operating systems). Therefore, it is not possible for the authorities to estimate the approximate extent to which an incident occurring at a particular vendor or service provider could spill over into the financial sector. Those that have this data have not yet analyzed the data; although it should be noted that the Operational Risk Division within OSFI has made some significant progress in collecting this data from 29 FRFIs and has undertaken some initial analysis of the potential concentration risk in their sector caused by dominant providers.

Furthermore, the CFRG conducted a cross-sector interdependencies analysis recently, which provided valuable insight to the FIs. Overall, the authorities would benefit from collecting this range of data and using the information and data to carry out analysis of interconnectedness in the financial system, understanding financial network exposures, and identifying the operational dependencies and critical nodes, which would thereby assist in managing potential systemic cyber risk. It should be noted that conducting interconnectedness analysis, as cited above, will further strengthen their ability to document additional and more detailed transmission channels and the different potential contagion scenarios.

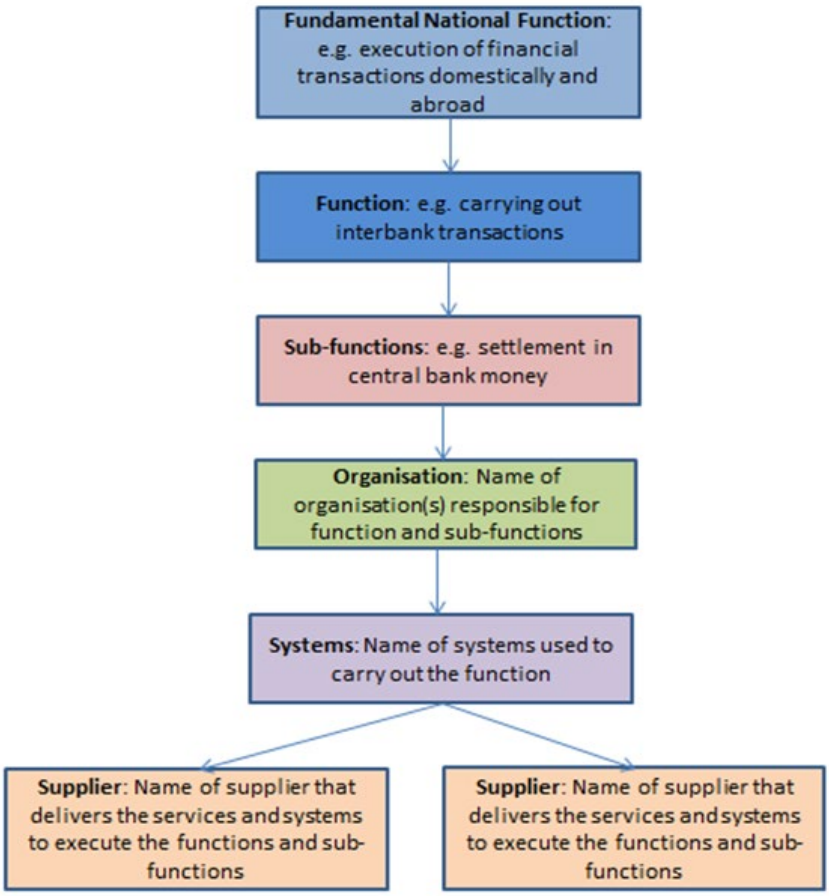
199. The authorities would benefit from deepening their analysis of the cyber interconnectedness of the financial system. It should be noted that analysis of the cyber interconnectedness, which some refer to as "cyber mapping", is an emerging field, with very few jurisdictions around the world having made any progress in its development. Analyzing 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 entity/service provider can spread to others. 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—could 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.

Recommendations

- The authorities should collect information and data of third-party providers and the technology being used by financial entities; they should use this data to conduct analysis of how the financial sector is operationally interconnected. This would entail developing network analysis of how the different critical sub-sectors are connected through common technologies and service providers, thereby allowing the identification of critical nodes. The authorities should use this analysis to:
    - Identify threats and their impact on the sector;
    - Develop a range of different scenarios that could threaten the sector(s) on a systemic level and develop mitigation strategies accordingly;
    - Conduct scenario-based tests or stress testing based on cyber scenarios; and
    - Improve incident response capabilities.

In developing the cyber map, the authorities could consider the approach described in Figure 3.

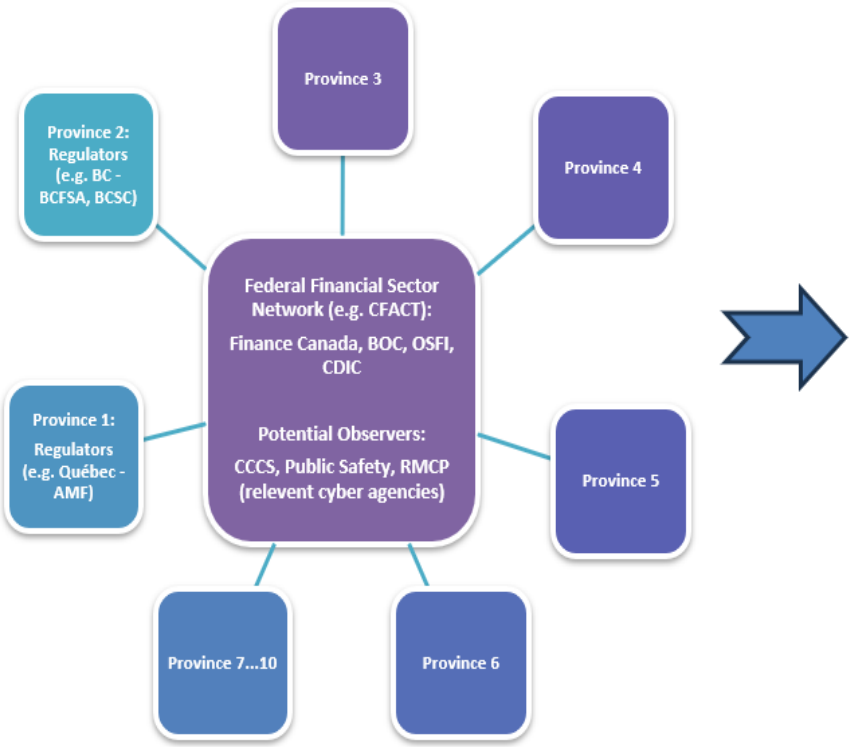
Figure 3. Canada: Structure of Possible Financial Sector Cyber Map



Source: IMF staff.

Annex I. Conceptual Example of "Financial Sector Network"

Figure I.1: Canada: Example of Potential Financial Sector Network



Areas of focus for coordination, cooperation and communication:

- Cyber Strategy
- Regulation/supervision
- Systemic crisis coordination and management
- Testing and Exercising
- Incident Reporting
- Public-private partnerships (e.g. CFRG)
- Information Sharing
- FINCERT
- Third party risk management
- Cross sectoral coordination
- Generic Threat Landscape
- Cyber Mapping

Source: IMF staff.