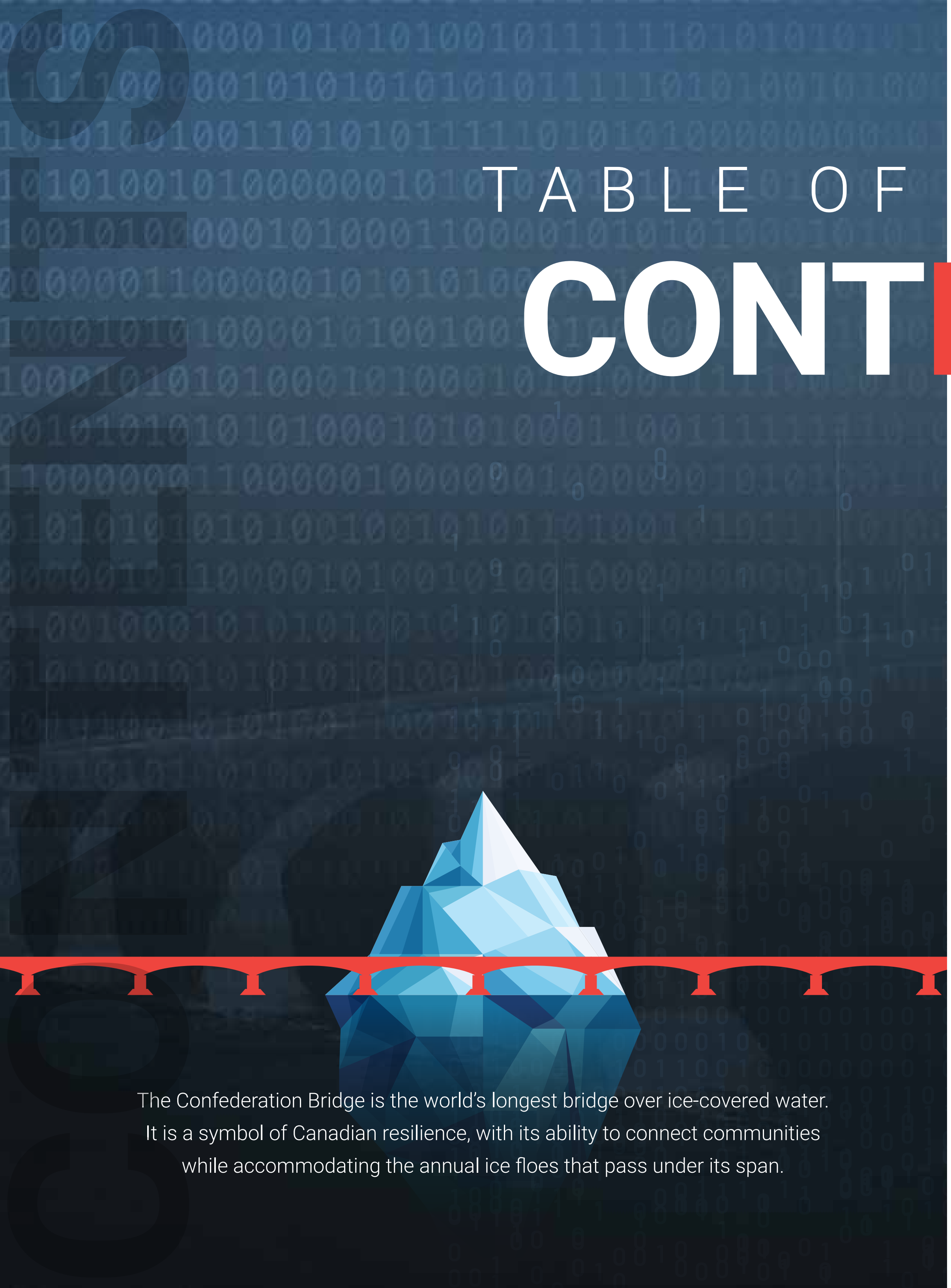
PAYMENTS CANADA

CYBER RESILIENCE STRATEGY

2022-2024

TABLE OF CONTENTS



The Confederation Bridge is the world's longest bridge over ice-covered water. It is a symbol of Canadian resilience, with its ability to connect communities while accommodating the annual ice floes that pass under its span.

MESSAGE FROM OUR PRESIDENT & CEO

Payments Canada underpins the Canadian financial system and economy by providing safe, efficient and effective clearing and settlement of payments. Key to our mandate is our cyber security program, which keeps Canada's payment systems safe and resilient against cyber threats.

This document explains Payments Canada's approach to cyber security: manage risk and foster preparedness and resilience within our organization and across the financial ecosystem. As we extend our security operating model across newly built payment systems in an evolving cyber threat environment, cyber security will continue to be a priority.

Our cyber security efforts not only keep Canada's payment systems safe from threat, but they also play a systemic role in keeping the Canadian financial industry secure. As we move into a new era of modern payments that support a vibrant economy, we look forward to continuing to collaborate closely with the Canadian financial community in promoting cyber security best practices and preparedness both nationally and around the world.

By meeting the challenges of today, we prepare to meet those of tomorrow.

Tracey Black
Payments Canada President & CEO

EXECUTIVE SUMMARY

Payments Canada's Cyber Security Vision:
We lead the payments world in cyber security.

Payment's Canada's Cyber Security Mission:
We keep safe the national payment systems and secure new payment methods.

Payments Canada forms a critical part of Canada's financial market infrastructure. We are responsible for the systems, processes and rules essential to payments clearing and settlement in Canada.

Our cyber resilience framework helps safeguard our organization and Canada's payment systems. The vision, mission and values that underpin our strategy help us stay focused on the safety aspect of our mandate.

Payments Canada implements a comprehensive Information Security Management System (ISMS) in line with the international standard ISO/IEC 27001:2013 (ISO 27001). An ISMS is a centrally managed framework that enables an organization to manage, monitor, review and improve information security practices. Payments Canada must meet the regulatory requirements for cyber security in accordance with the Bank of Canada's risk management standards, including the Guidance on Cyber Resilience for Financial Market Infrastructures. Internally, we have achieved tight alignment between our ISMS, systems security audits and broader management controls.

By implementing an ISMS and following the guidance, Payments Canada continuously monitors and improves upon a holistic program for cyber resilience. We also play a systemic role in keeping the Canadian financial industry secure by working directly with the Bank of Canada, financial regulators, the broader public sector, Canada's banks and the larger financial community. We help evolve cyber security standards to keep pace with threats. We engage deeply with our industry counterparts and lead regular cyber resilience exercises that ensure preparedness by confirming end-to-end cyber resiliency within the wholesale payment system.

Our cyber resilience framework encompasses our people, processes and technology — the three parts of an efficient whole. Five internal functions work together to protect corporate and payment system assets from cyber threats, while external cyber resilience objectives support our three organizational objectives: deliver, operate and facilitate.

GOVERNANCE & IMPROVEMENT

IDENTIFICATION & ASSESSMENT

PROTECTION & TESTING

DETECTION & AWARENESS

RESPONSE & RECOVERY

Payments Canada takes a leading role in keeping the Canadian financial industry safe from, and resilient to, cyber threats. Participating in industry forums and leading cyber resilience exercises are powerful ways to share knowledge and maintain alignment within the financial sector's cyber security community.

We are stronger together. This tight collaboration puts us in a good position to protect Canada's payment systems in coming years.

1. ISO Information Security Management standard
2. The Bank of Canada's risk-management standards
3. Bank for International Settlements, Committee on Payments and Market Infrastructures Guidance on cyber resilience for financial market infrastructures

CYBER RISK MANAGEMENT

We define risk as any variance against an expected outcome. Cyber incidents affecting payment systems, as well as the corporate systems that support them, are among the top enterprise risks that we monitor and manage at Payments Canada.

As part of our operational risk management program, cyber risk exposure is driven by both the impact and likelihood of an event and how effectively one or both of those factors can be mitigated. We evaluate the likelihood of cyber risk events as a function of the threats facing, and the control environment surrounding, critical assets.

The impacts of a material cyber event to Canada's payment systems would have systemic repercussions. We reduce the likelihood of risk events by continuously monitoring our threat environment and maturing our control coverage and effectiveness.

Payments Canada takes risks in accordance with our cyber risk appetite in order to achieve our legislative mandate and strategic objectives, but only if those risks position our organization and its systems to be among the most resilient within the global financial industry. We maintain an industry-leading security framework, with the supporting processes and tools that enable us to operate within this risk appetite.

Payments Canada defines its cyber risk tolerances through established thresholds within the risk appetite guidance and minimum acceptable performance measures. These tolerances are recorded in our operational procedures and summarized on a regular basis within our corporate reporting.

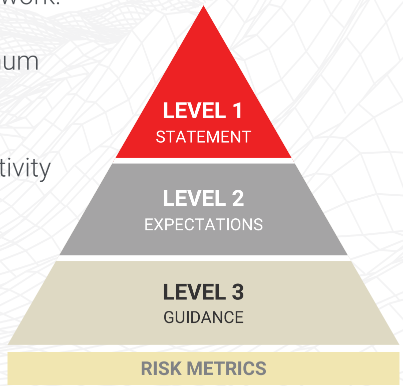
Payments Canada cyber risk appetite

LEVEL 1 We take risks to achieve our legislative mandate and strategic objectives only if those risks reinforce Payments Canada's position among the most cyber-resilient organizations in the global financial industry.

LEVEL 2 We maintain an industry-leading security framework.

LEVEL 3

- We operate a holistic ISMS and maintain minimum acceptable performance metrics.
- We maintain a clear understanding of the sensitivity of all our information assets and the security controls that apply to each.
- We monitor for and detect security issues in a timely manner and maintain minimum acceptable performance metrics.
- We respond to detected security issues in a timely manner and establish minimum acceptable performance metrics.
- We restore service to detected security issues in a timely manner and maintain minimum acceptable performance metrics.



CURRENT TRENDS

Our Cyber Resilience Strategy is informed by threat trends that evolve from a multitude of ever-accelerating changes in technology and business.

Industry trends of note include:

- **Big data analytics** An increase in massive stores of stolen credentials enable threat actors to mine and force passwords through authentication gateways in the hopes of a match. Additionally, massive stores of user information enable threat actors to analyze and understand victim behaviour with the intent to impersonate them in larger attack scenarios.
- **Artificial intelligence** The use of automation has increased the speed of cyber attacks. Cyber criminals are moving inexorably toward artificial intelligence and machine learning techniques; detection and response mechanisms now require corresponding improvements to remain effective.
- **Expanding perimeters** Organizational security perimeters continue to expand outward toward remote environments, including mobile devices and home offices. This notable change, stimulated by the advent of the coronavirus pandemic, highlights shifting opportunities for threat-actor targeting.
- **Quantum computing** The rise of quantum computing will accelerate progress in many fields of study and application. But when general-purpose quantum computers become available, it will also pose an existential threat to asymmetric cryptography.
- **Supply chain attacks** With an increase in cyber attacks on the digital supply chain, the world is seeing widespread and high-value breaches across entire sectors. The sophistication of supply chain attacks often implicates state sponsors with specific targets in mind.
- **Distributed cloud operations** The global coronavirus pandemic has hastened a steady shift toward cloud computing. This trend inspires a corresponding shift in workforce skills and security capabilities that leave lagging organizations behind in their ability to adopt new techniques to protect their assets.
- **Militarization of cyberspace** State-sponsored threat actors have launched targeted cyber attacks on central financial facilities for state gain. Sophisticated state-sponsored programs pose the greatest cyber threat to Canadian individuals and organizations.
- **Intelligence leaks** Occasionally, state-sponsored cyber programs either intentionally or unintentionally leak information or tools that become useful for criminal organizations. Two examples of this include:

  Data leaks. In recent years, anonymous entities have published hacking tools sourced from national intelligence agencies.

  Geopolitics. National intelligence agencies have been known to release cyber exploits in an effort to minimize the effectiveness of known adversaries. This also allows the private sector to develop fixes for the released exploits.
- **Criminal marketplaces** A sophisticated underground supply chain creates discrete products and services for threat groups. The commoditization of these tactics, techniques and procedures has enabled the procurement of pre-built cyber weapons for fast deployment.

OUR CYBER SECURITY JOURNEY

As cyber threats evolve, our cyber security posture also evolves to ensure that we continue safe and resilient operations. To reduce the impact and likelihood of cyber events, we constantly improve the way that we manage this risk.

Our cyber resilience framework, which lays out the functions, objectives and outcomes, reflects the increase in size and scope of Payments Canada's cyber security program. The framework supports our ability to monitor and evaluate our efforts to implement cyber security programs and reduce our risk.

In the last decade, we have improved the maturity of our security risk and governance practices. Keeping pace with industry maturation, Payments Canada has improved the integration of the cyber security program with our enterprise risk management framework. We also established different risk tolerances for payment systems versus corporate systems, with clear delineation between the two.

In 2017, we recruited a senior Chief Information Security Officer (CISO) to run our security program and regularly report to the Board of Directors, reinforcing the importance that Payments Canada places on cyber security. We have increased investments in cyber-related people, processes and technology in order to stay ahead of the evolving threat environment. We have grown a team of cyber security professionals and invested to further develop their knowledge, skills, and abilities with a focus on engagement and retention. We have also further developed our capabilities for continuously monitoring and responding to security events and engaged more closely with the financial industry in a number of work- and information-sharing initiatives.

We plan to continuously improve the cyber security functions to meet any new challenges facing our organization and the broader payments ecosystem. We will continue to monitor risks and adjust our corresponding risk treatments based on our risk appetite, member needs and regulatory guidance. As the world continues its shift toward cyber resilience, we will remain attuned to that shift while continuing to deliver on our mandate.

Our holistic approach to cyber resilience includes both a top-down look at business risks, taking into account the global threat landscape, as well as a bottom-up look at individual projects that change and protect our operating environment. From the top down, we continually improve our cyber security program with guidance from our regulators and in accordance with international best practices. We use key risks and research to prioritize the focus of those improvements and related projects. From the bottom up, we prioritize projects that increase business value while protecting the resilience of critical operations and assets. Between these converging approaches, we better manage cyber risks that could impair our ability to deliver on our cyber security mission.

2022-2024 CYBER SECURITY GOALS

Internal functions, long-term outcomes and strategic actions

We have enhanced our cyber resilience in recent years. We are focusing even more energy on the management of cyber risks anticipated in the years ahead.

The functions and objectives of this strategy combine to protect our corporate and payment system assets from cyber threats and to keep our national clearing and settlement systems safe and resilient.

GOVERNANCE & IMPROVEMENT

IDENTIFICATION & ASSESSMENT

PROTECTION & TESTING

DETECTION & AWARENESS

RESPONSE & RECOVERY

Payments Canada's cyber resilience framework supports our corporate goals. The framework is implemented through our ISMS, following Committee on Payments and Market Infrastructures (CPMI) guidance and adhering to ISO 27001.

This holistic international risk management–focused standard prescribes how cyber resilience objectives are determined and takes into account our people, processes and technology. Our internal functions and external cyber security objectives work together to address these three factors to fulfill our overall cyber security goals.

Goal 1: Deliver new financial systems and change programs in a safe and secure manner. This includes, notably, the Modernization program, including the delivery of a new high-value payment system (Lynx) and Real-Time Rail (RTR), as well as future initiatives.

Goal 2: Operate systems in a safe and sound manner by strengthening cyber resilience with attention to the people, processes and technologies that underpin the financial market infrastructures for clearing and settlement in Canada.

Goal 3: Facilitate improved resilience of Canada's payment systems by engaging with our stakeholders in sharing cyber security information and working together on cyber security initiatives. We share payments-specific threat intelligence with our members; we also lead and participate in cyber security–focused industry forums and groups. These forums include those within the Payments Canada Modernization program, the Canadian financial services collective, the Canadian Bankers Association, public/private partnerships and the credit union community.

2022-2024 CYBER SECURITY GOALS

Internal Function 1
Governance and Improvement

Establish clear roles, responsibilities and oversight mechanisms to support the implementation, review and continuous improvement of the Cyber Resilience Strategy and accompanying cyber resilience framework.

Long-term Outcomes:

- Defined roles and responsibilities for cyber resilience
- Independent audits and compliance reviews
- Alignment with ISO 27001 requirements
- Timely remediation of high-priority gaps

Strategic Actions 2022–2024

- **Undertake annual internal and external audits of the cyber resilience framework** in alignment with our ISMS implementation of ISO 27001, the international standard for information security management systems.
- **Remediate known gaps** by prioritizing risk and implementing mitigation measures to improve our cyber resilience posture and satisfy our regulatory obligations.

Internal Function 2
Identification and Assessment

Identify and manage corporate and payment system assets, including their dependencies on internal processes, procedures and systems, as well as their effect on external relationships.

Long-term Outcomes:

- Inventory and classification of business functions and processes
- Inventory and classification of information assets and dependencies
- Regular review and maintenance of asset inventories and related access
- Understanding the cyber risks to critical operations and ecosystem

Strategic Actions 2022–2024

- **Assess cyber maturity** by undertaking a triennial independent evaluation to understand cyber risks, identify gaps or weaknesses, promote strengths and aid in refining our roadmap of continuous improvement through management actions.

- **Continuously identify the risk of insider threats** within business functions and processes and create dynamic feedback for security controls against such threats. Elaborate on policy, governance and procedures for insider threat management, which will guide the requirements for further integration with technology controls.

Internal Function 3
Protection and Testing

Protect corporate and payment system assets against cyber threats by implementing and testing appropriate controls covering the associated people, processes and technology. This includes planning, developing and facilitating regular testing and exercises both internally and within the ecosystem to determine the overall effectiveness of the controls deployed to protect our critical assets, and leading initiatives to address prioritized gaps (if any).

Long-term Outcomes:

- Resilient systems, secured by design
- Appropriate and effective controls surrounding our assets
- Exercise roadmap with evolving methodologies and practices
- Ecosystem engagement in testing and exercise program

Strategic Actions 2022–2024

Improve Technical Controls

- **Build safe systems** that ensure participants meet the standardized security, attestation and compliance requirements of payment systems.
- **Increase network control maturity** by continuously improving the auditing and monitoring of our network and remediating any deficiencies.
- **Enhance cloud security controls** by improving security controls that allow for privileged access to remote services.

Improve Administrative Controls

- **Conduct penetration testing and remediation** on a regular basis. This consists of annual holistic security testing against Payments Canada infrastructure, as well as point-in-time security testing for any new Payments Canada capabilities or significant changes.
- **Conduct cyber resilience exercises** involving Payments Canada infrastructure and improve response capabilities to cyber incidents. We will also continue to coordinate participation in resilience exercises led by the Canadian Financial Sector Resiliency Group (CFRG). These are designed to improve responses and communications surrounding broader crises such as the coronavirus pandemic.
- **Improve assurance** by having a comprehensive and robust testing and exercise program for cyber resilience that also implements the lessons learned.
- **Improve identity and access management**, including key management controls and the maturation of our identity-governance mechanisms.

Improve Physical Controls

- **Improve access and monitoring controls** to Payments Canada premises and supporting facilities by continuously adopting the latest technology across alarm, surveillance and access systems.

Internal Function 4
Detection and Awareness

Detect cyber threats and incidents that impact, or have the potential to impact, our corporate and payment system assets by maintaining continuous monitoring capabilities. Actively participate in confidential threat intelligence activities to develop and sustain situational awareness to pre-empt cyber attacks.

Long-term Outcomes:

- Continuous monitoring of all key systems to detect anomalies
- Obtaining intelligence to identify potential cyber threats
- Exchanging timely information with trusted sources
- Supporting rapid response and containment activities

Strategic Actions 2022–2024

- **Enhance continuous monitoring and detection capabilities** to detect anomalous activities or behaviour in people, processes or technology associated with our key corporate and payment system assets.
- **Expand our security operating model** to incorporate vendors and partners, building a common operational picture and coordinated resources for cyber threat detection and response.
- **Enhance threat intelligence sharing** with trusted partners, including threat-actors' tactics, techniques, procedures and corresponding indicators of compromise.
- **Improve communication** of security threats and related awareness education to proactively mitigate potential issues.

Internal Function 5
Response and Recovery

Respond to cyber threats impacting corporate and payment system assets in a timely manner and recover from any incident or successful compromise. Integrate planning efforts with internal crisis management, business continuity and disaster recovery processes, as well as external service providers and ecosystem participants, as relevant.

Long-term Outcomes:

- Effective response to cyber security incidents that impact our assets
- Holistic and integrated capabilities to respond and recover
- Returning assets to their original state with enhanced controls
- Prioritized capabilities to promptly recover critical functions in a worst-case scenario

Strategic Actions 2022–2024

- **Implement 24/7 security operations capability** by maturing our round-the-clock security monitoring capabilities in terms of both personnel and alerting.
- **Support the development and testing** of enhanced contingency capabilities to augment existing tools and contingencies that may be leveraged in extreme but plausible scenarios.
- **Improve our understanding of security risk events** by ensuring consistency of root cause analyses, the holistic exploration of risk drivers, and timely follow-through on management actions.

2022-2024 CYBER SECURITY GOALS

Internal Plan

Internal Functions | Long-term Outcomes

GOVERNANCE & IMPROVEMENT	IDENTIFICATION & ASSESSMENT	PROTECTION & TESTING	DETECTION & AWARENESS	RESPONSE & RECOVERY
Defined roles and responsibilities for cyber resilience	Inventory and classification of business functions and processes	Resilient systems, secured by design	Continuous monitoring of all key systems to detect anomalies	Effective response to cyber security incidents that impact our assets
Independent audits and compliance reviews	Inventory and classification of information assets and dependencies	Appropriate and effective controls surrounding our assets	Obtaining intelligence to identify potential cyber threats	Holistic and integrated capabilities to respond and recover
Alignment with ISO 27001 requirements	Regular review and maintenance of asset inventories and related access	Exercise roadmap with evolving methodologies and practices	Exchanging timely information with trusted sources	Returning assets to their original state with enhanced controls
Timely remediation of high-priority gaps	Understanding the cyber risks to critical operations and ecosystem	Ecosystem engagement in testing and exercise program	Supporting rapid response and containment activities	Prioritized capabilities to promptly recover critical functions in a worst-case scenario

Internal Plan

Strategic Actions 2022-2024

GOVERNANCE & IMPROVEMENT

Undertake annual internal and external audits of our cyber resilience framework in alignment with our ISMS implementation of ISO 27001

Remediate known gaps by prioritizing risk and implementing mitigation measures to improve our cyber resilience posture and satisfy our regulatory obligations

IDENTIFICATION & ASSESSMENT

Assess cyber maturity by undertaking a triennial independent evaluation to understand cyber risks, identify gaps or weaknesses, promote strengths and aid in refining our our roadmap of of continuous improvement through management actions

Continuously identify the risks of insider threats within business functions and processes and create dynamic feedback for security controls against such threats. Elaborate on policy, governance and procedures for insider threat management, which will guide the requirements for further integration with technology controls

PROTECTION & TESTING

Improve technical controls

- Build safe systems
- Increase network control maturity
- Enhance cloud security controls

Improve administrative controls

- Conduct penetration testing & remediation
- Conduct cyber resilience exercises
- Improve assurance
- Improve identity & access management

Improve physical access controls to Payments Canada premises and supporting facilities by continuously adopting the latest technology across alarm, surveillance and access systems

DETECTION & AWARENESS

Enhance continuous monitoring and detection capabilities to detect anomalous activities or behaviour in people, processes or technology associated with our key corporate and payment system assets

Expand our security operating model to incorporate vendors and partners, building a common operational picture and coordinated resources for cyber threat detection and response

Enhance threat intelligence sharing with trusted partners, including threat-actors' tactics, techniques, procedures and corresponding indicators of compromise

Improve communication of security threats and related awareness education to proactively mitigate potential issues

RESPONSE & RECOVERY

Implement 24/7 security operations capability by maturing our round-the-clock security monitoring capabilities in terms of both personnel and alerting

Support the development and testing of enhanced contingency capabilities to augment existing tools and contingencies that may be leveraged in extreme but plausible scenarios

Improve our understanding of security risk events by ensuring consistency of root cause analyses, the holistic exploration of risk drivers, and timely follow-through on management actions

EXTERNAL OBJECTIVES

OUTCOMES & ACTIONS

The external objectives of the Payments Canada Cyber Resilience Strategy directly support our three organizational objectives: deliver, operate and facilitate. These objectives work together to support the safe, resilient and efficient operation of Canada's payment systems. Payments Canada's internal functions and external cyber security objectives, outcomes and actions are holistic in approach to ensure we successfully carry out our cyber security mission.

Strategic Actions 2022-2024

Objective 1: Deliver

Deliver new financial systems and change programs in a safe and secure manner

- **Engage the Canadian financial industry** on a regular basis to seek their advice and provide updates and reports on the development of security around evolving payment systems.
- **Engage with regulators** regularly to update them on cyber security plans and actions, and to secure approval for the cyber security strategies that we continuously evolve.
- **Engage with government**, especially for perspectives on the protection of supply chains required to develop and deliver secure payment systems. We also seek government partner support in collaborating with critical infrastructure partners on national security issues.
- **Secure new payments initiatives** from a cyber security perspective. For projects such as open banking, cross-border payments and other planned initiatives, we perform security assessments. These involve identifying sensitivities, threats and any potential mitigants required, and informing our stakeholders of risks. Ensuring the cyber security of new payments initiatives also involves implementing a plan that shapes initiatives in such a way that we can deliver on them safely and efficiently.

Objective 2: Operate

Operate all payment systems in a safe and secure manner

- **Manage authorized access** to payment systems. This involves ongoing support and evaluation of members' cyber security needs for system access.
- **Monitor payment systems** and partner integration points, and perform internal security monitoring and response as usual.
- **Share threat intelligence** with partners. For the planning period, as more new participants connect to Payments Canada's systems, we will continue enhancing and sharing threat intelligence with our stakeholders.
- **Seek attestations** in a process to independently validate member compliance with security requirements.

Objective 3: Facilitate

Improve the resilience of Canada's payment systems by facilitating engagement with our stakeholders

- **Facilitate public/private partnership** in information-sharing concerning payments-specific cyber threat intelligence.
- **Facilitate incident response planning** together with both the private and public sectors with respect to the designated payment systems.
- **Lead cyber resilience exercises** within the wholesale payment systems, including our people, our members, the Bank of Canada and integration points with other financial market infrastructures.
- **Improve internal/external intelligence** of specific threat-actor tactics, techniques, procedures and corresponding indicators of risk.

EXTERNAL OBJECTIVES OUTCOMES & ACTIONS

Cyber Resilience Strategy 2022–2024 | External Plan

External Objectives | Outcomes

DELIVER	OPERATE	FACILITATE
Deliver new financial systems and change programs in a safe and secure manner	Operate all payment systems in a safe and secure manner	Improve the resilience of Canada's payment systems by facilitating engagement with our stakeholders

Strategic Actions 2022-2024

DELIVER	OPERATE	FACILITATE
Engage the Canadian financial industry on a regular basis	**Manage authorized access** to payment systems	**Facilitate public/private partnership** in information-sharing concerning payments-specific cyber threat intelligence
Engage with regulators regularly to update them on cyber security plans and actions	**Monitor systems** and partner integration points, and perform internal security monitoring and response as usual	**Facilitate incident response planning** together with both the private and public sectors
Engage with government, especially for perspectives on the protection of supply chains required to develop and deliver secure payment systems	**Share threat intelligence** with partners	**Lead cyber resilience exercises** within the wholesale payment system
Secure new payments initiatives from a cyber security perspective	**Seek attestations** in a process to independently validate member compliance with security requirements	**Improve internal/external intelligence sharing** with Payments Canada internal business units and trusted partners

CONCLUSION

FROM VISION TO REALITY

The most critical role for Payments Canada is to ensure the continuous, safe operation of Canada's payment systems.

The Payments Canada Cyber Resilience Strategy outlines the path to achieving our mission, realizing our vision and accomplishing our goals by:

- Taking into account our people, processes and technology
- Following regulatory guidance and international best practices
- Pursuing the internal functions and external objectives that protect corporate and payments assets from cyber threats while supporting our organizational objectives

We deliver safe, efficient and resilient payment systems through the combination of an agile technology platform, a robust cyber security program, a strong risk culture within our capable and knowledgeable workforce, good governance and effective regulatory oversight from the Bank of Canada.

We continue to work closely on cyber resilience with our financial institution members, the Bank of Canada, the Department of Finance, key stakeholders and the broader public sector. Together we continue to effectively manage risk and security, building a financial system in Canada that is a model of cyber resilience.

Visit payments.ca to learn more about who we are and what we do.