Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada
Canada

GC Enterprise Cyber Security Strategy

Published: 2024-05-20

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT48-44/2024E-PDF
ISBN: 978-0-660-72248-1

This document is available on the Government of Canada website at www.canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Stratégie intégrée de cybersécurité du gouvernement du Canada

Government of Canada's Enterprise Cyber Security Strategy

On this page

Message from the President

Government of Canada Enterprise Cyber Security Strategy

The safety and security of Canadians is, and always has been, our top priority. Canadians rely on the Government of Canada to deliver programs and services, many of which are becoming increasingly more digital in this modern era. Like many public institutions around the world, the government has been a target of cyber-attacks, which can have a significant effect on government operations and the security of Canadians. We are constantly adapting safety measures and establishing tools to help safeguard our systems and protect Canadians' personal information.

Tools such as the Government of Canada's Cyber Security Event Management Plan, tabletop exercises, and government website security monitoring are proactive measures that help us anticipate and effectively respond to cyber events.

Now, we are taking additional steps to strengthen our approach and get a clearer picture of current cyber defenses across government. This first-ever Government of Canada Enterprise Cyber Security Strategy, developed by the Treasury Board of Canada Secretariat, Communications Security

Establishment Canada, and Shared Services Canada, is a risk-based, whole-of-government approach that will improve collaboration among departments and improve cyber security as a whole.

This Cyber Security Strategy is the first of its kind and is a testament to our commitment to keeping Canadians safe in the digital age. It will reduce redundancies, identify gaps, and include year-round testing and reviews.

It will also improve how the government prepares for, responds to, and recovers from cyber attacks, while fostering a diverse workforce with the right skills, knowledge, and culture to support cyber security. Canada's public service is one of the best in the world, and this Strategy will help ensure we have a workforce with the right tools to respond to complex cyber attacks.

Cyber security is an ongoing effort, and this strategy will be regularly reviewed and updated to ensure it keeps up with evolving threats.

Canadians can rest assured that the government is continuously implementing strong measures to safeguard their information and address cyber events when they do occur.

I invite you to read the Strategy to learn more about how the Government of Canada is strengthening cyber security across government.

The Honourable Anita Anand, P.C. M.P.
President of the Treasury Board

1. Introduction

▶ In this section

1.1 Context

Canadians rely on public institutions like the Government of Canada (GC) to deliver programs and services. As a critical infrastructure sector, government services are essential to the health, safety, security and economic well-being of Canadians. The increasing digital nature of the GC and reliance on information technologies means that the GC is an attractive target due to its holdings of personal information, valuable research data and other sensitive information.

As a result, cyber security events can have a significant effect on government operations, either through disruption of critical and essential services or through exposure of classified or personal information. This significant effect can put people at risk of identity theft or other types of fraud, all of which can potentially erode trust in government institutions and

negatively impact the overall Canadian economy and society. The *National Cyber Threat Assessment 2023–24* highlights the significant rise in the number and sophistication of cyber threat actors who take advantage of the dependency on Internet-connected technologies in order to conduct malicious activities. The increasingly complex threat landscape coupled with the rapid pace of technological innovation and adoption will make it even harder for GC departments and agencies to understand the risks they face and how they can and should protect themselves.

To that end, given the increasing sophistication and frequency of cyber attacks, the GC must remain vigilant and continue to strengthen its defences to improve resilience. Ensuring the confidentiality, integrity, and availability of the GC's information and networks is essential to the delivery of secure, reliable and trusted digital services. Enabling and maintaining a resilient digital GC will require a better understanding of the nature of the cyber risks along with action to modernize and secure systems to prevent and resist cyber attacks. When cyber events occur, the GC needs to be able to detect these events quickly to minimize their impact. Establishing a resilient cyber security posture will enable the GC to effectively respond to and recoverfrom cyber events in a timely manner to maintain the continuous delivery of government programs and services.

1.2 Purpose and scope

The purpose of the GC Enterprise Cyber Security Strategy (Strategy) is to:

- define the vision and strategic objectives for the GC that will keep pace with the evolving cyber security risk landscape, improve cyber security maturity and optimize GC cyber security investments
- develop a future state for the cyber security of government operations with supporting governance, oversight, and clear roles and responsibilities
- identify initiatives and requisite investments to support the implementation of the Strategy

The Strategy applies to departments and agencies under Treasury Board authorities, specifically under the *Policy on Service and Digital* and the *Policy on Government Security*. In addition, the scope of the Strategy is targeted for up to and including Designated (Protected B) information systems, along with Classified (Secret) information systems that focus on supporting government operations, while respecting the unique needs of the broader ecosystem of classified systems.

While federal departments and agencies not under Treasury Board authorities are not mandated at this time to apply and adopt Treasury Board policy requirements and direction, they are encouraged to adopt the

objectives and goals outlined under the Strategy to the greatest extent possible to improve cyber security posture across all government institutions.

1.3 Current environment

1.3.1 Drivers

> **Canada's Digital Ambition Statement**
>
> To enable delivery of government in the digital age for all Canadians. This will be done by providing modernized and accessible tools to support service delivery that expresses the best of Canada in the digital space.

As outlined in *Canada's Digital Ambition 2022*, today's digital landscape is marked by change of unprecedented pace and scope. Rapid technological, digital and data transformation is now part of Canadians' daily lives, revolutionizing the way they access information and services, and the way they live, socialize and work. Canadians expect to have faith in their government and to be able to access any government service, at any time and on any device, in a secure and accessible manner. However, meeting this expectation presents a variety of challenges and security considerations that must be reflected on as part of the ever-evolving cyber landscape, including:

- **Digital service delivery**
    - Canada faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector and ultimately Canadians' security and privacy.
    - As digital adoption increases, so do the opportunities for breaches and data loss. The growth in digitized personal information and improved delivery through digital approaches needs to be accompanied by measures to ensure that the privacy of Canadians will be protected and that government services can be delivered in the face of a rapidly evolving threat environment.
    - According to the Government of Canada Digital Standards: Playbook, services should be built to address the needs of users. Doing so includes applying a balanced approach to managing risk by implementing appropriate privacy and security measures that are frictionless so that they do not place a burden on users.
- **Environmental, social and governance (ESG) commitments**
    - As the GC increasingly focuses on responsible and sustainable digital service delivery, safeguarding its assets and Canadians'

personal information is integral to fulfilling the GC's social responsibility.
    - Environmental concerns highlight the need to minimize the carbon footprint associated with cyber attacks and data breaches, as these incidents often result in significant energy consumption.
    - Strong cyber security practices demonstrate a commitment to governance by upholding transparency, accountability and ethical conduct, and by reinforcing the reliability and trustworthiness of the GC among Canadians.
- **Future of work**
    - The COVID-19 pandemic has highlighted the need for more modern work tools and practices to support a hybrid work environment. Within days of the pandemic being declared in March 2020, most federal public servants began working remotely.
    - As measures were introduced to enable remote work during the pandemic, an expansion of risk tolerance was required to ensure continuity of government. Looking to the future, this risk tolerance and the related mitigations will need to be reviewed and realigned to reflect the new work environment.
- **Technology modernization**
    - Technology is evolving at an unprecedented pace, with new innovations and advancements being introduced regularly (for example, artificial intelligence (AI), quantum computing, blockchain). While this rapid evolution brings about many benefits and opportunities, it also creates additional threat vectors and new challenges for cyber security. The speed of technological change means that security measures that were once effective may quickly become obsolete, underscoring the need for a proactive and adaptive approach to cyber security, which is one where organizations are constantly evaluating and enhancing their security measures to keep pace with an ever-changing threat landscape. The speed of change causes difficulties in appropriate oversight, creating gaps in accountability and responsibility for cyber security risks.
    - The adoption and integration of Internet of Things (IoT) devices has led to the convergence of cyber and physical systems, which expands the attack surface where physical impacts can result from a cyber threat vector or where cyber impacts can result from a physical threat vector.
    - The manner in which information technology (IT) services are delivered and consumed has changed significantly in recent years

and is continuing to evolve. Widespread use of mobile devices and the adoption of cloud-based services are shifting the GC's technology environment and must be considered from a cyber security perspective.
    - While the traditional perimeter-centric security model has served the GC well, the notion that digital assets and users within a defined boundary are trustworthy does not scale to the "new digital world" where the trusted perimeter cannot be defined. Increased connectivity, the risk of insider threats, and the need to protect and store data in various in-house and third-party repositories (for example, cloud) have led to new security concepts that do not rely solely on a perimeter-centric security approach (that is, zero-trust).
- **Cyber security events and cyber security incidents continue to affect government**
    - Each year, there is an increase in the number of zero-day vulnerabilities that require immediate action from the GC.
    - Compromises within the supply chain (for example, SolarWinds) have an impact on the GC, and introduce operational risks when third-party services are used. There is a need for critical infrastructure institutions (that is, natural resources, financial, health, telecommunications) to be at the forefront of cyber security and resilience discussions during vulnerability analysis. The GC needs to ensure that all cyber security activities are conducted in conjunction with these critical infrastructure institutions to ensure a cohesive and collective approach to cyber security and resilience.
    - Sophisticated cyber incidents [1] affecting departments and agencies demonstrate that the GC continues to be a target, which drives the need to promptly address any architecture weaknesses in GC information systems.
    - Cyber attacks and data breaches also provide opportunities for fraudsters to exploit vulnerabilities and carry out fraudulent activities using techniques, such as social engineering, phishing, or enumeration of stolen credentials, to gain unauthorized access to systems that can potentially lead to identity theft or financial fraud.

1.3.2 Progress to date

Building and maintaining government cyber defences is therefore vital for the protection of the functions and services on which Canadian society depends. In the last decade, there has been progress made in improving the government's cyber security posture with centralized security capabilities having been implemented within the GC to some degree. Examples include:

- establishment of Shared Services Canada (SSC) as part of efforts to standardize the GC information technology (IT) infrastructure, including integration of cyber defence services at the GC enterprise perimeter
- establishment of the Canadian Centre for Cyber Security (Cyber Centre) as part of the Communications Security Establishment (CSE) to consolidate the operational cyber expertise from across the federal government and to provide a single, unified source of expert advice, guidance, services, and support on cyber security operational matters
- establishment of clear governance mechanisms to support the development of strategic cyber defence policy, the effective management of information technology security initiatives affecting government-wide operations, and the government response to cyber incidents
- increased availability of advice, guidance, and other tools and the implementation of minimum configuration requirements in 2022 as part of the *Policy on Service and Digital*, which was initially published in 2020, along with the renewal of the *Policy on Government Security* in 2019

1.3.3 Gaps remain

Despite this progress, gaps remain between the current state of government cyber resilience and where it needs to be. These gaps include:

- **Varying levels of cyber maturity**
    - The TBS Cyber Maturity Self-Assessment (CMSA) tool was launched in fall 2021 to support departments and agencies in assessing their cyber security maturity against recognized best practices, and is based on the methodology derived from the United States' National Institute of Standards and Technology (NIST) Cybersecurity Framework.
    - A year-over-year comparison of results from 2021–22 with results from 2022–23 demonstrates that departments and agencies are making marginal progress in improving their cyber maturity, and that they remain on average below the target of having repeatable processes to identify and respond to threats in support of an effective defence against new and emerging threats.
- **Lack of a comprehensive awareness of the cyber security risk environment**
    - The level of capability, investment, and security understanding across federal departments and agencies remains inconsistent. The size and complexity of the GC's digital estate, including the presence of legacy applications and technology, also make the challenge significantly more complicated.

    - Recognizing the potential gravity of impacts on the GC because of weaknesses in the supply chain, the increased use of third-party services has driven the need for more effective approaches and solutions to third-party risk management.
    - The ability to protect against evolving vulnerabilities and threats is further constrained by the presence of legacy GC information systems. This constraint drives the need to continue efforts in managing, upgrading or removing such systems, and in putting the necessary safeguards and ongoing investment in place to ensure that GC information systems are sufficiently secure throughout their entire life cycle. However, the tracking and maintenance of technology assets and data (both on-premise and in the cloud) are not comprehensively understood or managed, which limits visibility and awareness of which assets need to be protected. Many departments and agencies rely on manual processes, which can be time-consuming, error-prone and ineffective. The limits with regard to manual processes are particularly important for the many assets where proper tracking of configuration details (for example, exact cryptographic algorithms and their parameters) is needed.

- **Disparate approaches to and a lack of coordinated investment in various security capabilities can lead to inconsistencies, inefficiencies and blind spots in the GC's overall security posture**
    - Identity, credential and access management (ICAM)
        - Managing digital credentials in a manner that mitigates risks to personnel, organizational and national security, while protecting program integrity and enabling trusted citizen-centric service delivery is of utmost importance to the GC. To that end, there is a requirement to modernize current GC ICAM solutions to ensure that identity is managed consistently and collaboratively across the GC for both internal and external services, while also increasing the level of assurance that is needed to mitigate authentication threats.
    - Security monitoring
        - Departments and agencies are using a combination of different tools, methods and services to monitor their systems, which can make it difficult to obtain a comprehensive view of potential security threats and may lead to unintended duplication or gaps in monitoring. This difficulty drives the need for increased visibility and access to data to support end-to-end monitoring where departments and agencies can analyze data from their own unique operational perspectives. It

should be considered that many departments are not trained, equipped or staffed to support this function.

- While the scope of on-premise services is clear as it relates to the mandate (for example, SSC is mandated to provide email, network, and data centre services, and departments and agencies are responsible for endpoints and applications), the rapid adoption of cloud computing has resulted in a lack of clarity about roles and responsibilities and the extent to which existing roles and responsibilities are extended to the cloud. Due to this lack of clarity, departments and agencies have been expected to manage their cloud-based environments, including cyber security operations. This expectation has led to duplication of efforts, inconsistent approaches, lack of intelligence sharing, and reduced visibility for the GC enterprise with regard to cyber security event analysis and mitigation.

- Common services
  - While funding has been received to establish the enterprise cyber security capabilities, not all of these capabilities have been fully realized across the GC for various reasons, including waterfall approaches for project delivery and lengthy procurement processes.
  - The *National Security and Intelligence Committee of Parliamentarians' Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack* highlights the overarching challenge where government is increasingly managed horizontally while its foundational authorities remain vertical, which creates significant discrepancies. Specifically, Treasury Board policies intended to secure government systems are not uniformly applied given that:
    - individual departments and agencies retain considerable latitude over whether to opt into the framework or to accept specific defensive technologies
    - a large number of organizations, notably Crown corporations and potentially some other government interests, are not obligated to adhere to Treasury Board policies nor use the cyber defence framework
  - While the use of centralized services across government would help reduce enterprise risks, there is a need for increased information-sharing to support such use, including enhanced coordination in developing strategic, implementation and operational activities. This need is also magnified by the lack of

standardized tracking and service management of common services.

- **Traditional security architecture models are less effective as users and applications now exist outside the traditional network perimeter**
    - The growing threat of sophisticated cyber attacks has underscored that the GC cannot depend solely on conventional perimeter-based defences to protect critical systems and data. An information-centric approach where there is no implicit trust and all access is verified (also referred to as zero trust), coupled with host- and cloud-based network defence, will enable departments and agencies to rapidly detect, isolate and respond to these types of threats.
- **Misalignment between traditional approaches for security assessments and agile delivery methodologies**
    - As the GC moves toward working in a more agile environment with project management and development practices, security assessment and authorization (SA&A) processes in the GC continue to operate in a waterfall, compliance-based approach, which creates lengthy delays in the operationalization of information system solutions. The GC must evolve to a risk-based, threat-driven approach, which will reduce the friction with agile delivery methodologies while balancing security.
- **Weak information management practices**
    - Existing data protection processes are manual and have not comprehensively been standardized from creation to destruction. In addition, there is a lack of awareness of proper procedures related to the handling, processing, and classification of information (for example, under classifying or over classifying), resulting in inconsistent application across the GC.
    - There is inadequate protection of information due to outdated IT tools, which can result in an increase in cyber security incidents or privacy breaches, thereby eroding confidence in GC information management security.
- **Immature cyber security event management practices**

Cyber simulation exercises

Performing cyber simulation exercises (also referred to as tabletop exercises) helps to improve preparedness, enhance communication and decision-making, and provide cost-effective training that increases confidence in handling cyber security events. In 2021–22, only 25% of departments performed cyber simulation exercises.

  - While the GC has improved its central management of cyber security events through the establishment of the *Government of Canada Cyber Security Event Management Plan* (GC CSEMP), there is limited capacity within each department and it is not always clear which services provided at the enterprise level are available. Moreover, current solutions tend to be stand-alone and lack integration, workflow automation and the ability to generate trouble tickets to support cyber security incident management.
  - Departments and agencies experience a variety of significant or crisis events with varied complexity, and scope. They are responsible for identification, planning and recovery, as well as for the restoration of their critical services, internal operations, information systems and supporting applications. All these responsibilities are becoming more difficult to fulfill due to aging information systems and the increasingly distributed nature of technology assets. Sufficient resources are needed to ensure the continuity of critical services and to support incident recovery efforts.

- **Challenges related to people and culture of security**
  - The global demand for cyber talent far outweighs the supply, leading to a shortage of skilled professionals in the field. The GC is not immune, as vacant cyber positions continue to be a challenge for departments and agencies to staff. There is also a need to establish a right-sized staffing model for cyber talent between departments and central agencies so that positions are filled on a prioritized basis. The GC also has added layers of complexity due to security clearance requirements, second language profiles, and a hybrid work environment for many IT positions.
  - There is also a general lack of cyber security training available to GC personnel, both from a cyber domain perspective (for example, cloud security, incident response, security monitoring, use of existing cyber security tools) and from a general workforce perspective. To minimize cyber events that occur due to human

error, there is a critical need to upskill all personnel in order to drive cyber security leadership and knowledge across the GC as a whole.
    - Insiders with authorized access to sensitive data can pose a significant risk to the GC, through intentional or unintentional disclosure or misuse. Without modernized security screening and continuous assurance processes for employees and contractors, trusted and identity-based access to IT resources and information, and robust anti-fraud management practices, there is an increased risk of insider threat.

Addressing this ever-evolving cyber security risk landscape will require the GC to harness its collective strength to build secure and resilient information systems. This strength will be supported by action-oriented policies, increased agility, and strategic investment-planning focused on addressing gaps to ensure that Canadians remain confident that their data is protected and that the provision of critical services will be uninterrupted.

2. Whole-of-government approach for cyber security of government operations

▶ In this section

2.1 Vision

Enabling a whole-of-government approach for the cyber security of government operations that will support the delivery of government services in the digital age for all Canadians requires the GC to provide modernized and accessible tools that support service delivery. Cyber security is a foundational component that enables simple, secure, and efficient delivery of government services and benefits. Therefore, the GC must prioritize efforts in meeting its overall vision of:

> **Building a world-class, sustainable and resilient GC to reduce cyber security risks so that federal departments and agencies can enable secure and reliable digital service delivery.**

To realize this vision, the GC must prioritize efforts toward reducing cyber security risks so that GC departments and agencies can maximize the benefits of digital technology. This also means a concerted effort to optimize the use of its resources, leveraging common solutions where feasible to improve consistency and reduce the likelihood of misconfiguration. To do so, the GC will require the right policy, people, process, and technology to

identify and manage known and unknown or emerging risks, while maintaining a proportionate and effective level of cyber security across all federal departments and agencies.

This approach will also enable the GC to shift from a reactive posture to a proactive approach in identifying and addressing security vulnerabilities and capability gaps, while keeping pace with the rapidly evolving threat landscape. In addition, the GC must focus on safeguarding sensitive government data and ensuring that it protects and secures its information systems, regardless of their environments. Building in privacy and security from the outset and using an information-centric approach will enable the delivery of reliable services and support information systems that grant access to protected assets to trusted and verified users, devices, and services on a need-to-know basis.

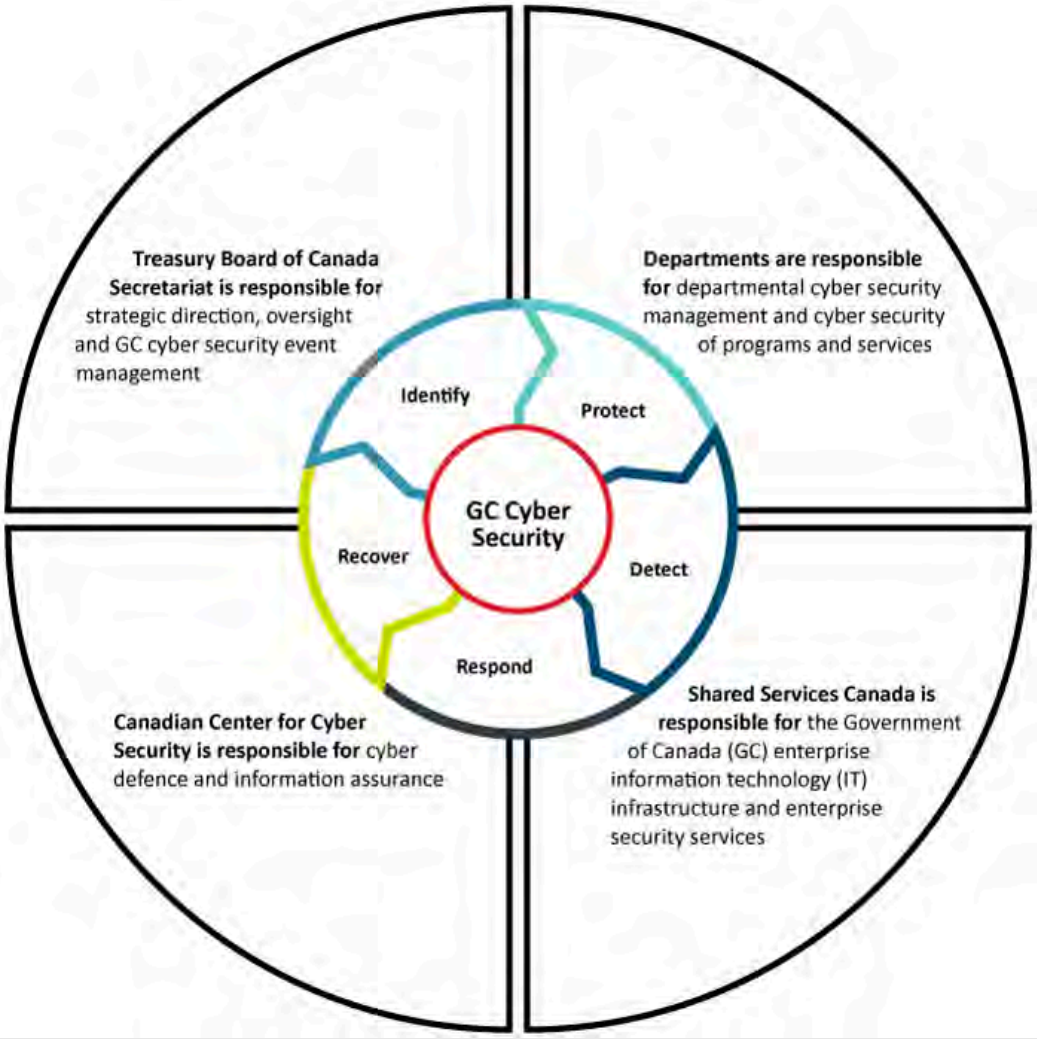
2.2 Key stakeholders

Cyber security management and coordination within the federal government is critical to ensure that the GC can stay ahead of cyber threats and provide the central leadership and support needed for Canada. Strengthened governance and oversight will be necessary to ensure collaboration and alignment with departments and agencies that fulfill a key role in managing cyber security. Every part of government has a role in achieving the vision.

To be successful, key stakeholders must work closely together. The key stakeholders include:

- **Treasury Board of Canada Secretariat:** Policy and oversight, strategic direction, GC cyber security event management
- **Communication Security Establishment and the Canadian Centre for Cyber Security:** Cyber defence and information assurance
- **Shared Services Canada:** GC enterprise IT infrastructure and enterprise security services
- **Departments and agencies:** Departmental cyber security management, including the cyber security of departmental programs and services

Figure 1: key stakeholders



▶ Figure 1 - Text version

Centrally, the Information Technology Security Tripartite (Tripartite), which consists of the Treasury Board of Canada Secretariat (TBS), Shared Services Canada (SSC), and the Canadian Centre for Cyber Security (Cyber Centre), plays an important role in providing advice, guidance, oversight, and direction to address GC-wide security initiatives, and supports departments and agencies under Treasury Board authorities. The Tripartite will continue its efforts to coordinate operational cyber security activities, transforming how cyber security data and threat intelligence is shared, consumed and actioned across government.

Departments and agencies are accountable for managing cyber security risks in their program areas; however, as the whole-of-government adopts an enterprise approach to cyber security and as programs and services become more integrated, it will be imperative that cyber security risks be effectively and holistically managed at the enterprise level in accordance with accountabilities outlined under the Treasury Board policy instruments.

Building on the expectations and authorities outlined under the *Policy on Government Security* and the *Policy on Service and Digital*, roles and responsibilities will be clarified as part of the target security operating model and its technology variations. Strong, collaborative relationships

between Departmental Chief Information Officers (CIOs), Departmental Chief Security Officers (CSOs), and the Designated Official for Cyber Security (DOCS) will be needed to:

- implement GC cyber security priorities and activities as part of the broader departmental security plans
- collectively ensure that departmental cyber security risks are managed to support the management of the overall cyber security risk posture

2.3 Strategic objectives

To realize the vision, four strategic objectives have been established along with supporting key actions. The objectives are:

- Articulate cyber security risks and their business impacts for effective, action-oriented and accountable decision-making
- Prevent and resist cyber attacks more effectively, leading to greater protection of Government of Canada (GC) information and assets
- Strengthen capabilities and resilience across the GC to proactively prepare for, respond to and recover from cyber security events
- Foster a diverse GC workforce with the right cyber security skills, knowledge and culture

These strategic objectives are further described in the section below. In addition, Appendix A: includes an initial set of key performance indicators to assess the progress of identified actions.

2.3.1 Objective 1: articulate cyber security risk and its business impacts meaningfully for effective, action-oriented and accountable decision-making

As the cyber threat landscape is complex, evolving and extremely sophisticated, the GC needs to increase its understanding of the cyber threat landscape in order to develop more comprehensive and layered security defences. In order to manage cyber security risk, federal departments and agencies will have risk management processes, governance, and accountability in place to enable the proactive and effective identification, assessment, and management of their cyber security risks. Multi-year departmental cyber security strategies will be submitted to the TBS Office of the Chief Information Officer (OCIO) for approval on an annual basis. Through this risk-based approach, there will be sufficient overarching visibility with access to data to drive analytics, enabling the GC to effectively manage and measure cyber security risk holistically and align mitigation strategies with GC-wide goals. Further, the GC will have the mechanisms in place to enable the rapid identification, assessment and management of vulnerabilities across the enterprise.

Key actions and goals include:

- **Plan and govern for the sustainable and integrated management of cyber security**
    - Define a common approach, methodology, solutions and tools for assessing GC cyber security posture that is aligned with GC policy and the IT governance context, and that applies a risk-based approach according to the Canadian Centre for Cyber Security's (Cyber Centre's) *IT Security Risk Management: A Lifecycle Approach* (ITSG-33).
    - Conduct independent assessments, ongoing (year-round) testing and comprehensive reviews of departments' cyber security posture to help identify and prioritize cyber security risks.
    - Strengthen governance related to digital and technology assurances, as part of the enterprise-wide IT investment-planning cycle, to ensure that cyber security spending proposals are aligned with government priorities and the Strategy.
    - Establish an integrated risk management platform that uses data-driven insights to identify, assess and communicate cyber security risks in a manner that:
        - resonates with senior management
        - provides actionable recommendations in order to improve risk remediation, prioritization of investments, and direction of resources
        - enables agile security assurance approaches
    - Ensure that resourcing and support is available to departments and agencies to improve their cyber security posture, in alignment with the Strategy and the target security operating model (TSOM).
- **Improve the understanding of GC-wide exposure and strengthen vulnerability management**
    - Implement tools to continuously identify, monitor, and manage the GC's attack surface, leveraging existing tools where possible.
    - Develop accurate asset inventories and map relationships and dependencies between assets, which will also facilitate patching efforts.
    - Proactively address infrastructure, system, and application vulnerabilities, and the cyber security risks they present with a GC Enterprise Vulnerability Management Program to ensure that identified vulnerabilities are effectively managed across the GC's digital estate, including building in redundancy and capability depth stemming from vulnerability assessments of our people, processes and technologies.
- **Enhance third-party cyber security risk management**
    - Seek measures to enhance system visibility and inventory management of the software and hardware supply chains to

protect GC information and assets as part of a robust third-party cyber security risk management approach.
    - Standardize and strengthen risk-based cyber security requirements, clauses, and conditions in contractual arrangements with external suppliers and perform routine verification of supplier adherence to contractual security clauses.

Expected outcome:

- **Cyber security is considered a whole-of-government endeavour where risks within GC information systems are continuously monitored, communicated, and remediated in an effective and timely manner**

2.3.2 Objective 2: prevent and resist cyber attacks more effectively leading to greater protection of GC information and assets

The GC relies on a range of technologies to operate its functions and deliver digital services, which fundamentally requires a security-by-design approach to ensure that the functions and services consistently and continuously follow best practices and meet robust standards. Moreover, federal departments and agencies will increase the use of shared capabilities, tools, and services to address common cyber security issues, improving cyber security across the whole of government, as well as driving efficiency and value for money.

Key actions and goals include:

- **Accelerate the implementation of modern cyber security and application architectures**
    - Modernize enterprise-wide identity, credential, and access management systems, including using multi-factor authentication everywhere, to enable the hybrid workforce.
    - Modernize applications and delivery methods using common reference architectures for the secure delivery of digital services.
    - Establish a secure-by-design approach with security architecture and engineering resources integrated within projects to ensure that security aspects and potential threats to the system are addressed.
    - Improve and standardize security assessment and authorization (SA&A) practices by sharing SA&A results across the enterprise to reduce duplication of efforts when assessing common components.
    - Continue expansion of cyber defence services for all federal departments and agencies to the greatest extent possible.
    - Transition GC systems to use standardized post-quantum cryptography to protect from the quantum threat.
    - Improve the GC’s ability to prevent, detect, respond to and recover from fraudulent activity against GC applications.

- **Deploy secure, modern, and accessible workplace tools and devices**
  - Deliver common and secure baseline endpoint solutions where feasible that consider the specific needs of the GC workforce, such as mobility, collaboration and accessibility. This includes:
    - establishing always-on protections that are aligned with GC policies, directives, standards, and guidelines and that are easily auditable to enhance trust across government
    - developing easy-to-use protection profiles and supporting playbooks that outline security requirements and a collection of required safeguards, which will enable the adequate protection of assets in alignment with the security categorization of the information and the threat environment
- **Strengthen data protection measures**
  - Improve information security practices with a refreshed security categorization model.
  - Establish automated data security policy enforcement to prevent unauthorized access and data loss.
  - Improve insider risk management and awareness to support continuous assurance and after-care practices.

Expected outcomes:

- **Standardized and modern tools, devices, and enterprise-wide cyber security services are deployed and leveraged across the GC**
- **A secure-by-design approach is applied to ensure that the security of digital services and protection of digital assets is continually assured throughout their life cycle**

2.3.3 Objective 3: strengthen capabilities and resilience across the GC to proactively prepare for, respond to and recover from cyber security events

Even with robust protection and detection measures in place, the GC will be impacted by cyber security incidents. It is therefore essential that the GC be able to rapidly respond to cyber security incidents when they do happen to minimize impacts and ensure the continuity of essential functions and services. Testing and exercising incident response plans, both organizationally and across government, as well as establishing the ability to identify and communicate lessons learned from incidents, is a key part of the approach. A holistic monitoring approach with proportionate security monitoring capabilities based on organizational size, business context and maturity will help to facilitate the proactive detection of cyber threats. Further, central oversight and support of recovery from the most severe cyber security incidents will ensure that systemic risks are identified and mitigated.

Key actions and goals include:

- **Improve security monitoring and detection capabilities to facilitate effective, tailorable options for departments and agencies**
  - Increase the clarity of roles and responsibilities pertaining to monitoring coverage among GC internal enterprise service organizations, departments and agencies.
  - Establish a federated security operations centre (SOC) architecture allowing for coverage that is commensurate with the operational needs of departments and agencies to increase efficiencies, minimize duplication of efforts and ensure effective coordination. Specifically:
    - A centralized or command SOC at the Cyber Centre that monitors the overarching GC security infrastructure (including on-premise networks, cloud environments and other endpoints) where departments benefit from the cyber defence ecosystem and gain access to their data via a security analytics platform.
    - A multi-function infrastructure security and network operations centre (ISNOC) at SSC to enable effective network monitoring for the well-being of core departments and agencies under SSC's mandate, along with the cyber security of common solutions provided by SSC, as well as to support the Cyber Centre and departmental security teams.
    - Specialized local SOCs for select departments and agencies that demonstrate sufficient maturity and that require additional visibility and nuanced metrics as a result of their unique mandates or business needs, which require enhanced monitoring to support the cyber security of program and service delivery.
    - Managed SOC services for departments and agencies that do not have sufficient maturity related to monitoring capabilities or resources, and that require hands-on coordination support.
  - Facilitate the sharing of logs and other critical information held at the enterprise-level to provide departments and agencies with end-to-end visibility of the data flows that support their information systems, which will enable departments and agencies to carry out their respective security responsibilities.
- **Enhance enterprise alignment with the *Government of Canada Cyber Security Event Management Plan* (GC CSEMP) to enable better preparation for, response to and recovery from cyber attacks**
  - Prepare departments through better incident planning and regular exercises using tools that allow for facilitated cyber simulation

exercises (also called tabletop exercises) and after-action reports shared centrally to support the prioritization of recommendations for GC-wide considerations. At minimum, departments and agencies will conduct one cyber tabletop exercise up to the Deputy Minister level each year.
    - Foster community collaboration enabled by a security incident response management platform to automate responses to and reporting of requests for action by departments and agencies.
    - Develop additional tools and templates to enhance departmental cyber security event management plan activities and support for the execution of the overarching GC CSEMP framework.
    - Establish rapid and scaled incident response and compromise recovery surge teams with various skill sets to support departmental recovery activities.
- **Improve the resilience of GC critical services with strengthened business continuity management practices**
    - Establish a GC-wide business continuity plan to ensure that there is a coordinated approach for managing events that affect multiple critical services in order to ensure the continued delivery of GC programs and services.

Expected outcomes:

- **GC networks, systems, applications, and endpoints are monitored to provide proportionate and end-to-end detection capability while respecting privacy**
- **GC information systems and critical services affected by cyber security incidents are quickly restored and resume operations with minimal disruption**

2.3.4 Objective 4: foster a diverse GC workforce with the right cyber security skills, knowledge and culture

To achieve the Strategy's vision and strategic objectives, the GC must cultivate a cyber security culture that empowers its people to learn, question and challenge in order to drive continuous improvement. Fostering a cultural shift in cyber security across the whole of government requires improving cyber security awareness and knowledge across all of the GC workforce in order to proactively engage organizational cyber security risks. According to the Government of Canada Digital Standards: Playbook, security measures should be frictionless so that they do not place a burden on users. Leveraging a robust cyber security culture across the GC will mature the cyber profession within the GC and enable the GC to attract,

develop, and retain those skills, and to provide sustainable career pathways more effectively. Doing so will also ensure increased awareness and vigilance among all GC employees.

Key actions and goals include:

- **Develop skills for cyber security**
  - Engage with relevant departments and agencies to implement cross-functional training programs to leverage a variety of learning solutions that upskill employees from different departments who have different levels of experience in cyber security in order to increase redundancies and strategic coverage to protect GC assets.
  - Establish standardized, mandatory cyber security awareness training across government for all of the GC workforce.
- **Attract and retain diverse talent for cyber security**
  - Establish strategic partnerships with educational institutions, industry groups, and other external organizations or communities to further improve proficiencies and gain practical experience that can be leveraged in the GC.
  - Establish a centre for cyber workforce development that will:
    - promote a talent management culture in which a principle objective is to recruit and retain those candidates with requisite cyber skills and expertise.
    - reduce duplication of effort, stimulate interdepartmental collaboration and knowledge-sharing for effective talent and resource development and retention.
    - support the establishment of clear career progression pathways for employees, including opportunities for advancement and increased responsibility, with a priority focus on promoting an inclusive workplace culture by leveraging GC-wide equality, diversity, and inclusion programs.
- **Accelerate the hiring of public servants by transforming personnel security screening and enabling continuous assurance**
  - Modernize personnel security screening with strengthened policy, automation and technology enablement.

Expected outcomes:

- **A cyber security culture across the entire GC that empowers behaviours that support continuous learning and improvement with a pool of cyber talent shared strategically across government**
- **A robust screening regime that balances evidence-based decision-making and continuous assurance to mitigate insider threat risks with improving the time it takes to hire**

2.4 Logic model

The following logic model has been created to illustrate the expected outcomes along key inputs and activities as well as the resulting outputs.

Table 1: logic model

Ultimate Outcome	A safe and resilient Canada					
Long-term outcome	A world-class, sustainable and resilient Government of Canada (GC) to reduce cyber security ris secure and reliable digital service delivery					
Intermediate outcome (5 to 10 years)	Departments and agencies use data-driven insights to articulate cyber risks and their business impacts to enable effective and accountable decision-making		Departments and agencies increase overall cyber maturity, leading to improved effectiveness in preventing and resisting cyber attacks	Departments and agencies put in place the capabilities required to proactively prepare for, respond to and recover from cyber security events		The GC wor composed that repres serve, and awareness all position
Immediate outcome (2 to 5 years)	Cyber security is a whole-of-government endeavour, where risks within GC information systems are continuously monitored, communicated, and remediated in an effective and timely manner	Standardized and modern tools and devices, and enterprise-wide cyber security services are deployed and leveraged across the GC	A secure-by-design approach is applied to ensure that the security of digital services and the protection of digital assets are continually assured throughout their life cycle	GC networks, systems, applications, and endpoints are monitored to provide proportionate and end-to-end detection capability while respecting privacy	GC information systems and critical services affected by cyber security incidents are quickly restored and resume operations with minimal disruption	A cyber security culture that empowers behaviors that suppor continuous learning an improveme with a pool of cyber talent share strategically across governmen

Outputs (2 years)	Integrated risk management platform GC Enterprise Vulnerability Management Program Standard security clauses in contracts to manage third-party risks	GC enterprise security architecture artifacts, tools and templates GC Identity, Credential, and Access Management (ICAM) strategy and roadmap Security playbooks Implementation of enterprise cyber security services	Target security operating model (TSOM) implementation artifacts Secure systems engineering and threat modelling practices Development, security and operations (DevSecOps) framework Modern security categorization model Digital data protection policies	Federated security operations centre (SOC) architecture Continuous monitoring framework Security monitoring use cases	Government of Canada Cyber Security Event Management Plan (GC CSEMP) playbooks Security incident response platform Facilitated cyber simulations (tabletop exercises) Incident recovery surge team Life-cycle framework for departmental business continuity management	Digital taler recruitmen and developme strategy Cyber Taler Centre of Expertise Cross-functional training programs
Activities (2 years)	Streamline governance, clarify accountabilities, develop functional capacity and tools, and measure cyber performance and maturity	Establish building blocks, develop guidance and deliver agile projects	Implement secure systems and development life cycles, and develop secure operating model processes	Develop requirements and use cases, clarify roles and responsibilities	Manage incidents, foster community collaboration, and establish and test business continuity and disaster recovery plans	Create, engage, an consult witl networks and partnership
Inputs (2 years)	Human and financial resources information from partners and stakeholders					

3. Implementation approach

To achieve the vision and meet the strategic objectives, a target security operating model (TSOM) is crucial in achieving an effective and efficient approach to conducting cyber security operations that enable the delivery of digital services. This model must consider the dimensions of policy, people, process, and technology, along with the GC's cyber security management

approach. This approach includes the security functions of identify, protect, detect, respond and recover that represent the primary pillars of a holistic cyber security program. The approach also provides guidance to departments and agencies to better understand, manage, reduce, and communicate cyber security risks, and complements existing practices outlined under the *Framework for the Management of Risk* and the Cyber Centre's *IT Security Risk Management: A Lifecycle Approach* (ITSG-33).

Therefore, the TSOM is an enabling tool to support the operationalization of the Strategy and provides a blueprint for successful cyber security operations. The TSOM illustrates the range of security processes and activities that are needed to have a comprehensive security capability, and provides a breakdown of stakeholders that are either accountable for or supporting each process and activity. Further, the TSOM provides a framework to clarify accountabilities and the extent to which additional authorities may be required to meet the target state for the cyber security of government operations.

Moreover, TBS, SSC, CSE, and departments and agencies will use the TSOM to guide the development of respective departmental plans that are aligned with this Strategy. These plans are expected to include an integrated investment-planning approach that incorporates cyber security and prioritizes the use of common solutions and enterprise services to the greatest extent possible where and when available. Departmental plans also support the establishment of departmental roadmaps. Such roadmaps include technology roadmaps that are developed by internal enterprise service organizations such as SSC as a key stakeholder in delivering secure, common solutions.

Monitoring and evaluation of the overall Strategy will be required to ensure that the vision and objectives of the Strategy are met. While the Tripartite will continue to play a key role in the governance and oversight of strategic initiatives, broader governance will also be necessary to oversee and obtain enhanced assurances as they relate to cyber investments. This broader governance, which will be built on TBS authorities that relate to spending oversight, will include early reviews of spending proposals to ensure alignment with the Strategy and government priorities. By establishing improved digital and technology assurances, the government will be enabled to operate in a holistic manner to promote the reuse of common solutions and technology, as well as to improve interoperability and efficient and collaborative asset utilization. Doing so benefits the government as a whole by helping to deliver savings and efficiencies, increase delivery confidence, reduce risk, support capability improvements and ensure improved outcomes for the GC.

4. Conclusion

While the GC has made progress in improving cyber security in recent years, the ever-evolving threat environment and evolution in technology has advanced even faster. A renewed commitment is required across departments and agencies to serve Canadians credibly and transparently in a manner that maintains and improves trust in the delivery of secure and reliable digital services. An appropriate balance between security, the associated cost and the end user experience is required. While security is of paramount concern, the GC must embrace a strong cyber risk culture to ensure that the necessary security controls commensurate with the sensitivity and value of the information are implemented in a cost-effective manner with minimal impact on the end user.

Appendix A: key performance indicators

The following table provides a proposed set of key performance indicators to monitor the progress of achieving the vision and strategic objectives outlined in the Strategy. These indicators will be further reviewed as part of the development of the supporting performance management framework for the Strategy.

Table A.1: strategic objectives, key actions and key performance indicators

Strategic objective	Key actions	Key performance indicators
Objective 1: articulate cyber security risk and its business impacts meaningfully for effective, action-oriented and accountable decision-making	Plan and govern for the sustainable and integrated management of cyber security	• Percentage of change in outstanding policy compliance issues for departments who completed their self-assessments
	Improve the understanding of GC-wide exposure and strengthen vulnerability management	• Understanding of GC-wide exposure is improved and vulnerabilities are mitigated: (1) to a limited extent; (2) to a moderate extent; (3) to a large extent
	Enhance third-party cyber security risk management	• Percentage of critical GC applications managed under the new software supply chain visibility and inventory management process • Percentage of GC-wide sampled contracts/contractors with verified adherence to cyber security contractual obligations

Strategic objective	Key actions	Key performance indicators
Objective 2: prevent and resist cyber attacks more effectively leading to greater protection of GC information and assets	Accelerate the implementation of modern cyber security and application architectures	• Percentage of departments who have adopted the agile SA&A process • Percentage of progress toward completion of GC post-quantum cryptographic transition plan • Percentage of departments onboarded to at least 1 of CCCS sensor services
	Deploy secure, modern, and accessible workplace tools and devices	• Secure, modern and accessible workplace tools and devices are deployed (1) to a limited extent; (2) to a moderate extent; (3) to a large extent
	Strengthen data protection measures	• Percentage of GC leveraging the updated Information Security Categorization Standard
Objective 3: strengthen capabilities and resilience across the GC to proactively prepare for, respond to and recover from cyber security events	Improve security monitoring and detection capabilities to facilitate effective, tailorable options for departments and agencies	• Percentage of departments that have implemented the use of the GC Security Monitoring and Operations Framework
	Enhance cyber security event management practices to prepare for, respond to and recover from cyber-attacks	• Cyber security event management practices are exercised across the GC: (1) to a limited extent; (2) to a moderate extent; (3) to a large extent
	Improve the resilience of GC critical services with strengthened business continuity management practices	• Applications that enable critical services across the GC are understood: (1) to a limited extent; (2) to a moderate extent; (3) to a large extent

Strategic objective	Key actions	Key performance indicators
Objective 4: foster a diverse GC workforce with the right cyber security skills, knowledge and culture	Develop skills for cyber security	• Percentage of GC personnel who completed their security awareness (mandatory) training year over year
	Attract and retain diverse talent for cyber security	• Percentage of reduction in the vacancy rate in GC cyber security roles
	Accelerate the hiring of public servants by transforming personnel security screening and enabling continuous assurance	• Median time to hire new public servants

Appendix B: glossary

critical service or activity

A service or activity whose disruption would result in a high or very high degree of injury to the health, safety, security or economic well-being of Canadians or to the effective functioning of the Government of Canada.

(Source: *Policy on Government Security*, Appendix B)

cyber security

Cyber security refers to the security of the transmission of electronic data and information across cyberspace. It covers the technology, processes, practices, and response and mitigation measures designed to protect electronic information, data and information infrastructure from mischief, unauthorized use or disruption in cyberspace. Cyber security complements IT security. Cyber security operationalizes the IT security controls set out in subsection B.2.3 of Appendix B of the *Directive on Security Management*.

(Source: *Guideline on Service and Digital*, subsection 4.6.1)

cyber security event

Any event, act, omission or situation that may be detrimental to government security, including threats, vulnerabilities and incidents.

Examples of cyber security events:

- disclosure of a new vulnerability
- intelligence that a threat actor may be planning malicious cyber activities against a GC information system
- attempts to breach the network perimeter
- suspicious or targeted emails with attachments/links that were not detected by existing security controls
- suspicious or unauthorized network activity that represents a deviation from baseline

(Source: *Government of Canada Cyber Security Event Management Plan* (GC CSEMP), subsection 1.5)

cyber security incident

Any event (or collection of events), act, omission or situation that has resulted in a compromise. Examples of cyber security incidents include:

- data breaches or compromise/corruption of information
- credential stuffing attacks
- phishing campaigns
- intentional or accidental introduction of malware to a network
- denial-of-service attacks
- web or online presence defacement or compromise (including unauthorized use of GC social media accounts)
- successful ransomware attempts

(Source: *Government of Canada Cyber Security Event Management Plan* (GC CSEMP), subsection 1.5)

cyber threat

An activity intended to compromise the security of an information system by altering the confidentiality, integrity, or availability of a system or the information it contains.

(Source: *Government of Canada Cyber Security Event Management Plan* (GC CSEMP), subsection 1.5)

information technology

Any equipment or system that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of information or data. It includes all matters concerned with the design, development, installation and implementation of information systems and applications.

(Source: *Policy on Service and Digital*, Appendix A)

insider threat

A malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems.

(Source: *National Cyber Security Strategy*, Workbook Glossary)

internal enterprise services

A service provided by a Government of Canada department to other Government of Canada departments intended on a government-wide basis.

(Source: *Policy on Service and Digital*, Appendix A)

IT security

IT security is the discipline of applying security controls, security solutions, tools and techniques to protect IT assets against threats from compromises throughout their lifecycle. IT security focuses on the security of both electronic data assets and physical IT assets. In other words, it covers, for example, the security of files that are stored on devices, the security of the systems used to store them and the security of the devices themselves.

(Source: *Guideline on Service and Digital*, subsection 4.6.1)

vulnerability
Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

(Source: *Government of Canada Cyber Security Event Management Plan* (GC CSEMP), subsection 1.5)

zero-day exploit
An attack directed against a zero-day vulnerability.

(Source: *Government of Canada Cyber Security Event Management Plan* (GC CSEMP), subsection 1.5)

zero-day vulnerability
A software vulnerability that is not yet known by the vendor, and therefore has not been mitigated.

(Source: *Government of Canada Cyber Security Event Management Plan* (GC CSEMP), subsection 1.5)

Footnotes

1 Canada's foreign affairs department targeted in "significant" cyber attack, *National Post*, January 24, 2022; Canada's National Research Council hit by "cyber incident", *Globe and Mail*, March 21, 2022; DDoS attacks block PM Trudeau's web site, *IT World Canada*, April 11, 2023

ISBN: 978-0-660-72248-1