Government of Canada
Gouvernement du Canada

Canada.ca › Shared Services Canada › Publications and reports

Audit of Cyber and IT Security Governance

Table of contents

Background

Cyber security is a shared responsibility between Shared Services Canada (SSC), the Canadian Centre for Cyber Security (CCCS), Communications Security Establishment (CSE), Treasury Board of Canada Secretariat (TBS) and partner organizations. Among these organizations, SSC, CCCS, and TBS are collectively known as the GC IT Security Tripartite (Tripartite). The Tripartite organizations carry out specific government-wide responsibilities and services, including for the narrower mandate of cyber defence.

SSC, as the Government of Canada (GC) IT service provider, continues to focus on strengthening cyber security, and defending the GC IT infrastructure from network-based attacks, malicious software, and other cyber threats. Cyber attacks have become increasingly frequent and threat actors are leveraging sophisticated technologies such as Artificial Intelligence (AI) to discover and exploit vulnerabilities in GC systems. As the level of sophistication of cyber threats increases, SSC must evolve to strengthen cyber security capabilities needed to manage the cyber threat landscape.

SSC is subject to the Treasury Board (TB) *Policy on Service and Digital* and the TB *Policy on Government Security* that set out cyber security and IT security requirements for departments and agencies. SSC has further defined roles and responsibilities for cyber and IT security in the *Policy on Departmental Security*, the *Directive on Departmental Security*, and the *Directive on Security Management for Enterprise Services*.

SSC has a two-fold approach to cyber and IT security, as defined in its policy instruments:

- enterprise security services: cyber and IT security services provided by SSC to GC departments; and

- corporate security services: internal services that create a safe and secure environment ensuring the protection of individuals in the workplace and of information and assets under departmental control, and enabling continued delivery of departmental programs and services [1].

To strengthen enterprise security services, SSC, under the leadership of the Chief Technology Officer (CTO), will be developing a Cyber Security Program in collaboration with the Senior Assistant Deputy Minister, Network and Security Services Branch (NSSB). The Cyber Security Program will enhance cyber security governance and capability, and continuously evolve the GC’s enterprise security posture to better meet business needs and address emerging threats. At the time of the audit, the Cyber Security Program had not been established. Responsibility for the program and associated cyber security responsibilities, however, have been delegated to the CTO since 2022.

Objective, Scope and Methodology

Objective

The objective of this audit was to provide assurance on: the effectiveness of the governance structure; that roles and responsibilities relating to cyber and IT security were defined, documented, communicated and well-understood throughout the Department; and that cyber and IT security were integrated into core business lines, including service management, enterprise architecture and cloud operations.

Scope

The scope for this audit addressed both corporate and enterprise services, and included:

- SSC’s cyber and IT security governance framework;
- the effectiveness of decision-making;
- policy and direction;
- the accountabilities, roles, and responsibilities for managing SSC’s cyber and IT security functions;
- integrated cyber and IT security planning;
- cyber and IT security risk management; and
- oversight, including monitoring and reporting.

The audit covered the period from January 1, 2022, to September 30, 2023.

The scope excluded cyber and IT security-related operational functions such as patch management, vulnerability management, Security Assessment and Authorization (SA&A), and IT continuity planning, as these areas were covered in recent audits.

Methodology

The audit was conducted by means of:

- Interviews with senior management and operational staff with cyber and IT security roles and responsibilities;
- Interviews with selected cyber and IT security Committee and Board members;
- Review of documentation, including records of decision, agendas, and presentation material for each of the cyber and IT security Committees

and Boards;
- Review of cyber and IT security risk management practices; and
- Identification of key controls.

Statement of conformance

This audit engagement was conducted in conformance with the Institute of Internal Auditors' *International Professional Practices Framework* and the Treasury Board of Canada *Policy on Internal Audit*, as supported by the results of the Office of Audit and Evaluation’s quality assurance and improvement program.

Observations

Audit observations were developed through a process of comparing criteria (the correct state) with condition (the current state). Where applicable, recommendations were made regarding conditions that were noted as areas of improvement. An overall audit conclusion was also made against the audit objective.

The observations, recommendations, and conclusion of this internal audit engagement were reported to senior management and the SSC Departmental Audit Committee.

Management response

Management has agreed with the findings and accepted the recommendations of this internal audit. Where applicable, the Chief Technology Officer Branch, the Enterprise IT Procurement and Corporate Services Branch, the Networks and Security Services Branch, and the

Strategy and Engagement Branch have developed action plans to address findings and recommendations, the implementation of which will be monitored by the Office of Audit and Evaluation.

Lines of enquiry and criteria

Line of enquiry 1: Governance

1.1 SSC has an effective oversight regime in place to manage cyber and IT security risks and issues:

a. SSC has defined the structure of governance bodies to effectively manage cyber security risks and issues;
b. SSC has integrated cyber and IT security governance into the management of key enterprise activities (cloud, service management, project management, and enterprise architecture); and
c. senior management has sufficient information to make cyber and IT security decisions in a timely manner.

1.2 SSC has developed, documented, and communicated a policy instrument including cyber and IT security:

a. policy instruments are up-to-date and include corporate and enterprise cyber and IT security activities; and
b. policy instruments are in compliance with the GC policy framework.

1.3 SSC roles and responsibilities for cyber and IT security are appropriately defined, documented, communicated, and maintained up-to-date:

a. roles and responsibilities between SSC and its partners (Tripartite, customers) for enterprise are clear, documented and communicated;
b. SSC roles and responsibilities for cyber and IT security are aligned across all functional areas (corporate and enterprise);

c. SSC has designated the role of the Departmental Official for Cyber Security (DOCS) as per the TB Policy on Service and Digital, and how it relates to the rest of the policy framework in the department; and
d. responsibilities and accountabilities for cyber and IT security incidents and event management are defined, coordinated, documented, communicated, and understood by all stakeholders who have a role in cyber and IT security.

1.4 SSC has developed a departmental cyber security plan that has been approved by senior management:

a. the plan addresses a Cyber Strategy, a Cyber Security Program, roadmaps, and action plans; and
b. cyber security planning has been integrated into other areas of planning (i.e., infrastructure, data, service, procurement, and capacity management).

Line of enquiry 2: Risk management

2.1 SSC has implemented a risk management process that accurately reflects cyber and IT security risks, including the establishment of risk tolerance levels required to identify priorities in support of decision-making.

Line of enquiry 3: Monitoring and reporting

3.1 SSC has implemented appropriate monitoring and reporting mechanisms that include:

a. compliance with SSC and GC policies;
b. key cyber and IT security metrics that are reported regularly to senior management and monitored; and

c. a standardized set of triggers and tools that have been implemented to ensure reporting is accurate and complete.

Footnote

[1] Definition extracted from the SSC Policy on Departmental Security - Appendix A

Date modified:
2025-07-08