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

Audit of IT Security – Phase I

Published: 2025-09-22

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

Catalogue Number: BT66-101/1-2025E-PDF
ISBN: 978-0-660-79018-3

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Audit de la sécurité des TI – Phase I

Audit of IT Security – Phase I

On this page

Results at a glance

▶ In this section

Significance

The Treasury Board of Canada Secretariat (TBS) supports a Cabinet Committee and its role as a central agency. Therefore, good information technology (IT) security practices are paramount to safeguarding its personal and sensitive information holdings.

Objective

Assess the effectiveness, adequacy and compliance of TBS's IT security activities in identifying, addressing and mitigating vulnerabilities and threats.

Scope

Review of relevant TBS IT security activities between August 2022 and November 2024.

Observations

Overall, there are no findings that pose significant or severe risks to TBS's operations or information holdings. However, there were a few areas where management could focus their attention to improve effectiveness or alignment with government-wide policies.

Recommendation

- It is recommended the Assistant Secretary, Corporate Services Sector and Chief Financial Officer review and update, as necessary, select policy and procedure documents to ensure completeness and alignment with government-wide policy instruments or the department's system development life cycle.

Without updated policy and procedure documents, Internal Audit and Evaluation Bureau's ability to assess compliance and operational effectiveness of some IT security-related controls will be limited in future planned engagement over the next few years.

Considerations

In addition to the recommendation, there are two additional areas raised for management's consideration to improve effectiveness:

- Assigning a departmental committee as a forum to more routinely share information or seek input on IT security matters with senior management
- Reviewing how information is organized in the department's inventory of applications

Context

The Government of Canada's Enterprise Cyber Security Strategy makes it clear that "The increasing digital nature of the Government of Canada (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." Furthermore, it states, "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." [1]

Given that TBS supports a Cabinet Committee and its role as a central agency, good IT security [2] practices are paramount to safeguarding its personal and sensitive information holdings.

In the last five years, TBS's IT security practices have evolved and adapted with the shift to more cloud-based services, such as Microsoft 365 (M365), and to remote and hybrid working arrangements for its employees.

This is the first IT security audit conducted by the Internal Audit and Evaluation Bureau (IAEB) to reflect this shifting to cloud-based services. Given that IT security covers a vast array of activities, IAEB plans to conduct additional IT security-related engagements over the next few years.

Engagement overview

This audit reviewed activities from August 2022 to November 2024 related to the following areas of focus:

- IT security governance (roles and responsibilities)
- IT security policy framework
- IT security planning and performance measurement
- IT security risk management
- IT security user awareness and training
- secure system acquisition and development (security assessment and authorization process)

See Appendix A for more details on the scope and methodology of the engagement.

Results

Overall, there are no findings that pose significant or severe risks to TBS's operations or information holdings. However, there were a few areas where management should focus their attention.

Area of focus	Observations	Impact	Recommendation
Roles and responsibilities and policy framework	While the department had the required policy framework documents, some of the documentation was outdated and did not adequately reflect all the roles of key individuals such as the designated official for cyber security. Even with outdated departmental documentation, key individuals understood their roles and responsibilities as they related to the government-wide policy instruments.	There is a risk that: • gaps in responsibilities may exist, and that the key individuals may be unable to adequately fulfill their mandates or that they may apply their roles and responsibilities inconsistently • employees lack awareness and understanding of their roles and responsibilities	It is recommended the Assistant Secretary, Corporate Services Sector and Chief Financial Officer review and update, as necessary, the • departmental IT security policy framework documents • security assessment and authorization process documents to ensure completeness and alignment with government-wide policy instruments or the department's system development life cycle.

Area of focus	Observations	Impact	Recommendation
Security assessment and authorization (SA&A) * process	While the department had a documented process, it did not clearly articulate how this process aligned with the department's system development life cycle. Furthermore, some documentation was outdated and did not reflect all the roles of key individuals in this process.	There is a risk that: • gaps in responsibilities may exist, and that the key individuals may be unable to adequately fulfill their mandates or that they may apply their roles and responsibilities inconsistently • employees lack awareness and understanding of their roles and responsibilities	It is recommended the Assistant Secretary, Corporate Services Sector and Chief Financial Officer review and update, as necessary, the • departmental IT security policy framework documents • security assessment and authorization process documents to ensure completeness and alignment with government-wide policy instruments or the department's system development life cycle.

Area of focus	Observations	Impact	Recommendation
*	SA&A: IT security assessment and authorization processes – Process to establish and maintain confidence in the security of information systems that are used or managed by the department, while considering stakeholder security requirements Appendix B: Mandatory Procedures for Information Technology Security Control (*Directive on Security Management*) (B.2.6)		

In addition, there are areas for management consideration to improve its effectiveness.

Area of focus	Observations	Impact	Consideration

Area of focus	Observations	Impact	Consideration
Governance	While there is no policy requirement, it is a good practice to have regular IT security discussions with senior management. There is no designated departmental management committee to discuss IT security matters (such as, risks, issues, priorities) on a periodic basis. It was noted that IT security matters are presented and discussed on an ad hoc basis at senior management committee meetings.	A lack of regular discussions regarding IT security at senior management level may lead to inadequate prioritization of activities, lack of departmental awareness of risks and mitigation measures to implement, and insufficient information for decision making.	Management might consider assigning a departmental committee as a forum through which key individuals such as Chief Information Officer or Designated Official for Cyber Security can: • provide information, on a regular basis, to senior management regarding IT security matters • seek input, when required, to assist in the fulfillment of their responsibilities to provide department-wide strategic leadership, coordination and oversight on IT security matters.

Area of focus	Observations	Impact	Consideration
Security assessment and authorization (SA&A) process	While the department has and maintains an inventory of its applications, how the information is captured and organized is not conducive to monitoring results of the SA&A process nor to tracking remediation actions of outstanding vulnerabilities.	There is a risk that key vulnerabilities may not be addressed in a timely manner. In addition, management may limit its ability to effectively plan future activities, monitor for trends, or identify potential department-wide vulnerabilities.	Management might consider reviewing how information is organized in the application inventory to ensure that key information needed for decision-making and monitoring can be easily retrieved.

For the results of other areas assessed during the audit, refer to Appendix B.

For the Management Action Plan Response, refer to Appendix C.

Appendix A – About the engagement

▶ In this section

Authority

The audit engagement was identified in the approved Treasury Board of Canada Secretariat (TBS) 2021–22 TBS Integrated Audit and Evaluation Plan (IAEP).

Statement of conformance

This audit engagement was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing. [3]

Objective and scope

The audit objective was to assess the effectiveness, adequacy and compliance of TBS's IT security activities in identifying, addressing and mitigating vulnerabilities and threats.

The focus for Phase 1 was to evaluate the effectiveness of the TBS:

- IT security governance (roles and responsibilities)
- IT security policy framework
- IT security planning and performance measurement
- IT security risk management
- IT security user awareness and training
- secure system acquisition and development (SA&A process)

The above scope of the audit was driven by the result of a risk assessment [4] and took into consideration work performed by other advisory and assurance providers to avoid duplication.

The audit period covered relevant TBS IT security activities between August 2022 and November 2024.

The audit scope did not include:

- a review of TBS's Enterprise Resource Planning (ERP) systems [5]
- Controls that reside outside of TBS's area of responsibility, including controls performed by Shared Services Canada

Methodology

The audit approach and methodology were risk-based and conformed to the International Standards for the Professional Practice of Internal Audit. Engagement methodologies included:

- Review of applicable Treasury Board and departmental policy instruments and procedures for the management and administration of the IT security function
- Review of key documentation (for example, governance documentation, IT security policy framework, IT security strategy, standard operating procedures, training, awareness campaigns)
- Interviews with key partners in the Information Management and Technology Directorate staff
- Process walkthroughs (for example, governance structure, policy framework, SA&A process)
- Testing of controls (for example, SA&A process)

Appendix B – Lines of enquiry, accompanying audit criteria and overall results

Line of enquiry 1 – A framework is in place that adequately details the accountabilities, policies, planning and reporting requirements necessary to ensure that IT security risks are mitigated.

Criteria	Results	Recommendation / consideration
1.1 Governance and roles and responsibilities. A governance framework for IT Security has been established, and includes defined roles and responsibilities, planning and investment oversight, and third-party relationship management, to ensure the identification and mitigation of IT security risks.	• Minor issue in area identified – outdated policy documents • Opportunity regarding additional oversight based on good practices	• Recommendation 1 • Consideration 1
1.2 Policy framework. The IT security policy framework ensures that required IT security controls are applied consistently and are appropriately communicated.	• Minor issue in area identified – outdated policy documents	• Recommendation 1
1.3 Planning and performance measurement. There is a comprehensive, risk-based, IT security plan that includes performance monitoring and vulnerability management.	• No issues identified.	• None identified.

Criteria	Results	Recommendation / consideration
1.4 Risk management. There is a process to proactively identify, assess and mitigate IT security risks.	• No issues identified.	• None identified.
1.5 Awareness and training. IT security training and awareness activities are provided, aligned to policy and tailored to different users.	• No issues identified.	• None identified.

Line of enquiry 2 – TBS has implemented processes and controls to mitigate IT security risks related to the acquisition and development of systems.

Criteria	Results	Recommendation / consideration
2.1 Security assessment and authorization (SA&A) process. There is a process to identify and mitigate IT security risks and vulnerabilities in a timely manner, as required.	• Minor issue identified in area – outdated procedure documents • Opportunity to enhance information recorded as part of the inventory	• Recommendation 1 • Consideration 2

Appendix C – Management action plan

▶ In this section

To support the review and updating of key IT security-related documents, management was asked to identify a response and action plan to address the recommendation identified.

Items for management's consideration are points to take into account in decision-making and will not be included as part of the IAEB's follow-up process. As such, no management response and action plan was sought.

Recommendation

It is recommended the Assistant Secretary, Corporate Services Sector and Chief Financial Officer review and update, as necessary, the:

- departmental IT security policy framework documents
- security assessment and authorization process documents

to ensure completeness and alignment with government-wide policy instruments or the department's system development life cycle.

Management response

We agree with the recommendation.

Proposed actions for recommendation	Start date	Targeted completion date	Entity responsible
1. Update IT security policy framework documents	June 2025	September 2025	Manager, IT Security

Proposed actions for recommendation	Start date	Targeted completion date	Entity responsible
2. Update the security assessment and authorization (SA&A) process documents	June 2025	September 2025	SA&A Technical Advisor

Management consideration

We recognize the benefits of having a governance committee assigned as a forum for IT security matters and, while not required, have created an action plan for the following item for management's consideration.

Management might consider assigning a departmental committee as a forum through which key individuals such as Chief Information Officer or Designated Official for Cyber Security can:

- provide information, on a regular basis, to senior management regarding IT security matters
- seek input, when required, to assist in the fulfillment of their responsibilities to provide department-wide strategic leadership, coordination and oversight on IT security matters.

Management response

We agree with the consideration.

Proposed actions for recommendation	Start date	Targeted completion date	Entity responsible
1. Create a TBS IT Committee a. This committee will have as one mandate overseeing IT Security Reporting. b. This committee will report to the Investment and Human Resources Committee within the TBS Committees Governance structure and provide a minimum of quarterly updates to that committee.	July 2025	September 2025	Chief Information Officer

---

1 GC Enterprise Cyber Security Strategy

2 While cyber security is considered a subset of IT security, for the purpose of this report IT security and cyber security are used interchangeably.

3 The engagement was started/conducted under the old IPPF (standards prior to January 2025) and as such this report was drafted using those standards.

4 A comprehensive risk assessment was undertaken of all IT security areas based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

5 The IT controls for the ERP systems are audited annually and reviewed periodically through the Internal Control over Financial Management (ICFM) Framework.

ISBN: 978-0-660-79018-3

Date modified: 2025-10-03

xx
yy