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

Canada

Coordinated Audit of Information Technology Security (with Shared Services Canada)

Published: 2018-01-05

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

Catalogue Number: BT66-80/2018E-PDF
ISBN: 978-0-660-43955-6

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 coordonné de la sécurité de la technologie de l'information (avec Services partagés Canada)

Coordinated Audit of Information Technology Security (with Shared Services Canada)

ℹ **Note to readers:**

This report contains information severed in accordance to the Access to Information Act.

Table of Contents

Statement of conformance

The Internal Audit and Evaluation Bureau has completed the Coordinated Audit of Information Technology (IT (information technology)) Security. This audit conforms with the Internal Auditing Standards for the Government of Canada, as supported by the results of the Bureau's quality assurance and improvement program.

Executive summary

Background

This audit was part of the Treasury Board of Canada Secretariat's approved Risk-Based Audit Plan for 2014 to 2017. It was conducted to provide additional assurance not covered within the scope of a recent Horizontal Audit of IT (information technology) Security in Large and Small Departments performed by the Office of the Comptroller General of Canada.

The Government of Canada has adopted a "defence in depth" [1] approach to managing IT (information technology) security in order to protect its data and systems. This approach is based on multiple layers of security measures aiming to prevent and lessen the potential exploitation of vulnerabilities.

Shared Services Canada and the other lead security agencies (the Government of Canada's Chief Information Officer Branch, Communications Security Establishment Canada, and Public Safety Canada) coordinate IT (information technology) security activities to secure the government's network perimeter from external threats. This coordination includes implementing necessary security measures as well as monitoring the activities on the government's network. The departmental Secretariat network is located behind the government's network perimeter.

This audit examined the adequacy of the IT (information technology) security controls in place to protect the Secretariat's network and infrastructure. Given the distributed responsibility for IT (information technology) security controls and the required coordination with Shared Services Canada, the internal audit groups of the Secretariat and of Shared Services Canada took a coordinated audit approach to provide broader assurance.

Objective and scope

The audit's objective was to assess the adequacy and effectiveness of internal controls over the management of departmental IT (information technology) security, including compliance with applicable policies and standards.

The audit scope focused on the services and business processes that have the highest potential impact on IT (information technology) security for the Secretariat and for which a high degree of collaboration or coordination between Shared Services Canada and the Secretariat is required.

Processes pertaining to software development, access to business applications, and the Government of Canada Secret Network were excluded from the scope of the audit.

The audit procedures were initiated in September 2015 in order to leverage work performed as part of the Office of the Comptroller General of Canada's Horizontal Audit of IT (information technology) Security. The examination phase was completed in August 2016.

Audit results

The audit focused on four key aspects of managing the Secretariat's IT (information technology) security: user access management, incident management, change management, and information security risk management. The audit team concluded, with a reasonable level of assurance, that the controls over the management of departmental IT (information technology) security were in most respects adequately designed and effective.

While the results were positive overall for areas where the Secretariat has the authority to action, the audit identified certain controls that should be strengthened [This information has been severed] to fully mitigate risks to an acceptable level. These controls relate to those that are internal to the Secretariat, as well as to the need for improved coordination and collaboration between the Secretariat and Shared Services Canada.

Specifically, the following points apply:

- Processes are in place to properly identify and classify servers that store sensitive information. In addition, users generally have the appropriate access rights to perform their duties. [This information has been severed]
- Departmental processes are in place to monitor network activities for security incidents. [This information has been severed]
- Information owners and information system owners have key roles and responsibilities for aspects of IT (information technology) security. [This information has been severed]
- Opportunities exist to establish a risk-based approach for the timely transformation of Secretariat services to the Shared Services Canada end state [This information has been severed]

[This information has been severed] recommendations have been made to support improvement of internal controls over the management of departmental IT (information technology) security at the Secretariat.

Management response

The Secretariat has developed a management response and action plan, which is presented in Appendix A.

[This information has been severed]

1. Introduction

The Treasury Board of Canada Secretariat is the administrative arm of the Treasury Board. The Secretariat assists the Treasury Board in setting the rules that establish how people, public funds and government assets are managed; in managing the government's expenditure plans and the stewardship of public funds; in considering and recommending regulatory changes that impact the health, safety and security of Canadians, the economy and the environment; and in determining the terms and conditions of employment for the core public administration. [2] This assistance is provided by over 1,700 employees [3] who access information on the Secretariat's network based on the core security principles of "least privilege," "need to have" and "need to know."

The creation of Shared Services Canada in 2011 brought together people, technology resources and assets from 43 federal departments and agencies to improve the efficiency, reliability and security of the government's IT (information technology) infrastructure. Beginning November 15, 2011, Shared Services Canada assumed responsibility for email, data centres and network services for the Secretariat (the IT (information technology) infrastructure). Maintaining the Secretariat's IT (information technology) security posture became a shared responsibility between the Secretariat and Shared Services Canada.

A coordinated audit approach was adopted to assess the IT (information technology) security posture for areas of shared responsibility. The coordinated approach allowed each department to examine the IT (information technology) security activities conducted under its respective department and responsibility, and to assess the activities through every step of the process without being hampered by organizational boundaries. The results were shared between the internal audit functions of both departments, but each will report the results for their own organizations.

1.1 Organizations

The Government of Canada has adopted a "defence in depth" [4] approach to managing IT (information technology) security in order to protect its data and systems. This approach is based on multiple layers of security measures aiming to prevent and delay the potential exploitation of vulnerabilities.

Shared Services Canada has the mandate to provide data centres, networks and email services to 43 federal departments and agencies (partner organizations). Shared Services Canada, Communications Security Establishment Canada, and Public Safety Canada have a shared responsibility for cyber and IT (information technology) security, with oversight provided by the Secretariat and supported by the Chief Information Officer Branch. These organizations coordinate IT (information technology) security activities to secure the government's network perimeter from external threats. This includes implementing necessary security measures as well as monitoring the activities on the government's network. The departmental Secretariat network is located behind the government's network perimeter.

The audit examined the adequacy of the IT (information technology) security controls in place to protect the Secretariat's network and infrastructure.

Maintaining a robust internal IT (information technology) security posture requires continued vigilance from the Secretariat's Corporate Services Sector, with the cooperation from and coordination with Shared Services Canada.

The audit focused on the activities of the Information Management and Technology Directorate of the Secretariat's Corporate Services Sector.

Given the distributed responsibility for IT (information technology) security controls and the required coordination with Shared Services Canada, the internal audit groups of the Secretariat and Shared Services Canada took a coordinated audit approach to provide broader assurance.

2. Audit details

2.1 Authority

The Coordinated Audit of Information Technology Security is part of the Secretariat's approved Risk-Based Audit Plan for 2014 to 2017.

2.2 Objectives and scope

The audit scope focused on the services and business processes that have the highest potential for impact on IT (information technology) security for the Secretariat and for which a high degree of collaboration or coordination between Shared Services Canada and the Secretariat is required, specifically:

- user access management
- IT (information technology) security incident management
- management of changes that have a potential IT (information technology) security impact
- IT (information technology) security risk management

Audit procedures were applied to activities performed between April 1, 2014, and June 2015. Evidence produced outside this time frame was also considered. The IT (information technology) security activities performed by Shared Services Canada on the behalf of the Secretariat were reviewed and assessed by the Office of Audit and Evaluation of Shared Services Canada, and are presented in a separate report.

The audit was launched in February 2015, with audit procedures initiated in September 2015 in order to leverage work performed as part of the Horizontal Audit of IT (information technology) Security by the Office of the Comptroller General.

2.3 Scope exclusions

The audit excluded the following:

- **Software development:** Limited software development activities are performed by Shared Services Canada for Secretariat systems; therefore, these activities were assessed as low risk and scoped out of this audit.
- **Access to business applications:** Access to business applications, including non-standard software, was not included in the scope of the audit because of the absence of coordination required between Shared Services Canada and the Secretariat in this process.
- **Government of Canada Secret Network:** The Government of Canada Secret Network was excluded from this audit [This information has been severed]. The Office of the Comptroller General of Canada had identified classified

information management as a risk area identified for future consideration [5] as a separate audit.

2.4 Approach and methodology

The audit approach and methodology were risk-based and conformed with the Internal Auditing Standards for the Government of Canada. These standards require that the audit be planned and performed in such a way as to obtain reasonable assurance that the audit's objectives were achieved.

The audit included various tests and procedures considered necessary to provide such assurance, including the following:

- interviews with key personnel at Shared Services Canada and the Secretariat
- documentation review
- walk-throughs
- control testing
- substantive testing
- data analytics

2.5 Lines of enquiry

The audit had four lines of enquiry:

- **User access management:** The Secretariat's information is protected against unauthorized access to maintain the level of information security risk acceptable to the Secretariat in accordance with applicable security policy instruments and procedures. Information security roles and access privileges are established and maintained, and security monitoring is performed.
- **IT (information technology) security incident management:** Timely and effective response to potential information security incidents is provided. Incidents are recorded, investigated, diagnosed, escalated and resolved.
- **Management of changes that have a potential IT (information technology) security impact:** IT (information technology) system changes that impact security are managed in a controlled manner. Such changes include change

standards and procedures, security impact assessment, prioritization, authorization, emergency changes, tracking, reporting, closure and documentation.

- **IT (information technology) security risk management:** IT (information technology) security risk exposure is continually assessed and reduced within levels of tolerance set by management in collaboration with Shared Services Canada.

The audit criteria were derived from the Control Objectives for Information and Related Technology, version 5.0 (COBIT (information technology) 5) and the ISO/IEC 27001: Information security management standard.

The audit criteria used to assess each line of enquiry are presented in Appendix B.

3. Audit results

The audit results are presented by line of enquiry.

[This information has been severed]

Overall conclusion

The audit team concluded, with a reasonable level of assurance, that the controls over the management of departmental IT (information technology) security were in most respects adequately designed and effective.

While the results were positive overall for areas where the Secretariat has the authority to action, the audit identified certain controls that should be strengthened across the four areas of audit scope in order to fully mitigate risks to an acceptable level. These controls relate to those that are internal to the Secretariat and to the need for improved coordination and collaboration between the Secretariat and Shared Services Canada.

[This information has been severed] recommendations have been made to support improvement of internal controls over the management of departmental IT (information technology) security at the Secretariat. They are presented in Appendix

A, along with management's actions to address them.

Appendix A: management response

[This information has been severed]

Appendix B: audit criteria

[This information has been severed]

Footnotes

[1] Government of Canada IT (information technology) Strategic Plan for 2016 to 2020, Secure IT (information technology)

[2] Treasury Board of Canada Secretariat Departmental Performance Report for 2015 to 2016

[3] Population of the Federal Public Service by Department: Treasury Board of Canada Secretariat

[4] Government of Canada Information Technology Strategic Plan for 2016 to 2020, "Secure IT (information technology)"

[5] Office of the Comptroller General of Canada Risk-Based Audit Plan for 2016 to 2019, Appendix H: Risk Areas Identified for Future Consideration

Date modified:

2018-01-05