Public Services and Procurement Canada
Services publics et Approvisionnement Canada

Canada

Serving GOVERNMENT, serving CANADIANS.

Audit of IT Security - summary

Office of the Chief Audit Executive

Table of Contents

Introduction

1. This engagement was included in the Public Services and Procurement Canada (PSPC) 2018 to 2021 Risk-Based Audit and Evaluation Plan.

2. PSPC plays an important role in the daily operations of the Government of Canada as a key provider of services for federal departments and agencies. Many of the services provided by PSPC are enabled by information technology, which in a fast evolving global technology environment, is an increasing source of risk to the confidentiality, integrity, and availability of information, and the systems on which the Department depends to operate.

3. Treasury Board Secretariat is responsible for establishing policy, direction, and guidance for protection of government programs and services, along with the people, information and assets, that support them. Baseline security requirements are outlined in the *TBS Policy on Government Security and Directive on Security Management.* The Policy requires each department to establish a security program for the coordination and management of departmental security activities, including that for IT.

4. At PSPC, through the '*Departmental Security Program'* policy, the Deputy Minister has delegated the overall administration of the Departmental Security Program to the Assistant Deputy Minister, Departmental Oversight Branch. The responsibility for the direction of the Departmental Security Program (including its development, implementation, maintenance and monitoring) has been delegated to the Departmental Security Officer, who is also the Director General, Security Emergency Management Sector, Departmental Oversight Branch.

5. One of the requirements of the Departmental Security Program is to have an IT Security Program. The administration of the IT Security Program is under the responsibility of the Digital Services Branch. The development, management and direction of the IT Security Program is delegated to the Director, IT Security Directorate in Digital Services Branch (who is also the Departmental IT Security Coordinator).

Audit Objective

6. The objective of this internal audit was to provide assurance that key control activities to mitigate IT security risks within PSPC are designed, implemented and operating as intended.

Audit Scope and Approach

7. The scope period of this audit engagement was from April 1, 2017 to March 31, 2019. Audit fieldwork for this audit was substantially completed on May 30, 2019.

8. The audit covered activities of the Digital Services Branch-managed network and other networks on which PSPC IT assets reside, and included processes and controls for IT security at headquarters and in the regions.

9. The criteria for this internal audit engagement were derived from the Treasury Board Secretariat's *Policy on Government Security, Directive on Security Management, and Operational Security Standard on Management of Information Technology Security*; the National Institute of Standards and Technology Cybersecurity Framework 1.1; the

Communication Security Establishment's Top 10 and ITSG-33; and the PSPC Departmental Policy on IT Security.

Observations

10. Audit observations were developed through a process of comparing criteria (the correct state) with condition (the current state). Audit observations noted satisfactory performance, where the condition meets the criteria, or they may note areas for improvement, where there was a difference between the condition and the criteria. Where applicable, recommendations were made toward conditions that were noted as areas of improvement. An overall audit conclusion was also made against the audit objective.
11. The observations, recommendations, conclusion of this internal audit engagement were reported to the senior management and the PSPC Departmental Audit Committee.

Management response

12. Management agrees with the findings and accepts the recommendations of this internal audit. Where applicable, the Departmental Oversight and Digital Services Branches have developed action plans to address findings and recommendations, the implementation of which will be monitored by the Office of the Chief Audit Executive.
13. PSPC is committed to ensuring that the key control activities to mitigate IT security risks are designed, implemented and operating as intended.

Statement of Conformance

14. The audit conforms with the *Internal Auditing Standards* for the Government of Canada, as supported by the results of the quality assurance and improvement program.
15. Sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the findings and conclusions in this report and to provide an audit level of assurance. The findings and conclusions are based on a comparison of the conditions, as they existed at the time, against pre-established audit criteria that were agreed on with management. The findings and conclusion are only applicable to the entity examined and for the scope and time period covered by the audit.