Health Canada and the Public Health Agency of Canada
Santé Canada et l'Agence de la santé publique du Canada
Canada

Summary Document

Audit of Information Technology (IT) Security at the Public Health Agency of Canada and Health Canada

March 2017

1. Background

Information Technology (IT) is a strategic asset and critical enabler of the Government of Canada's commitment to deliver integrated and easily accessible services to Canadians, while ensuring that internal administrative operations are managed efficiently and effectively. The Treasury Board of Canada Secretariat (TBS) *Operational Security Standard: Management of Information Technology Security* (MITS) defines IT Security as the "safeguard" to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information. For the purposes of this audit, "IT Security" refers to anything involving the security of electronic information regardless of media, including cybersecurity.

Corporate administrative services, which include IT services, are managed under the Shared Services Partnership Framework Agreement between Health Canada (HC) and the Public Health Agency of Canada (PHAC). Under this Agreement, the Information Management Services Directorate (IMSD) of the Corporate Services Branch (HC) is responsible for the implementation and maintenance of the end-user IT infrastructure (e.g., desktop computing). IMSD is also responsible for the development and maintenance of software applications supporting programs and services. Currently the departmental IT security function falls within the purview of the Executive Director of IT Service Delivery. Accountability for all aspects of security, including IT security, rests with the Departmental Security Officer (DSO). The IT Security Coordinator (ITSC) is responsible for the management of the IT security program.

Corporate administrative services, which include IT services, are managed under the Shared Services Partnership Framework Agreement between Health Canada (HC) and the Public Health Agency of Canada (PHAC). Under this Agreement, the Corporate Services Branch (HC) is responsible for providing security services. Accountability for all aspects of security, including IT security, rests with the Departmental Security Officer (DSO). The IT Security Coordinator (ITSC) is responsible for the management of the IT security program.

There are also a few IT systems in HC and PHAC that do not come under the purview of the IMSD or SSC. These are systems that have been deployed and are operated inside both organizations that are not managed by IMSD. The Science Network at the Radiation Protection Bureau, under the Healthy Environments and Consumer Safety Branch at HC and the Bioinformatics Network at the National Microbiology Laboratory (NML) in Winnipeg, under the Infectious Disease and Prevention and Control Branch at PHAC are examples of IT networks that are separate from and do not interface with the HC and PHAC corporate network.

2. Audit objective

The objective of the audit was to assess the effectiveness of the management control framework for managing IT security in HC and the PHAC and to ensure the compliance with TBS and departmental policies, directives and standards.

3. Audit scope

The scope of the audit included an examination of key practices and processes in place for managing IT security and the level of technical and operational safeguards that exist in HC and PHAC. The audit included a review of IT infrastructure, IT services, departmental applications and systems, and the management of electronic information under the control of HC and PHAC.

IT infrastructure and services provided by Shared Services Canada (SSC) and other third party service providers were excluded from the audit since they are not under the control of HC and PHAC. The scope of the audit also excluded IT continuity for mission-critical applications/systems, personnel and physical security, as well as safeguards around paper-based records, as these topics were recently covered in other audits.

The audit covered the period from April 1, 2015 to September 30, 2016.

4. Audit approach

The audit examined the governance, risk management and control practices for managing IT security in HC and PHAC against a set of pre-defined audit criteria. The audit approach included a review of documentation, policies, standards, guidelines, frameworks and business processes. Interviews have been conducted with key officials from CSB and the NML. Interviews were also conducted with the Departmental Security Officer (DSO) and other departmental officials from program areas. The audit reviewed roles, responsibilities and accountabilities for managing IT security in HC and PHAC. Lastly, the audit performed testing, analysis and review of internal IM/IT controls to ensure that key IT security controls were present for managing departmental IM/IT assets. The audit was carried out in the National Capital Region and in Winnipeg.

5. Findings

Recommendations were issued in the areas of governance, risk management and control. Management has a management response and action plan in place to address the recommendations.

6. Statement of conformance

In the professional judgment of the Chief Audit Executive, sufficient and appropriate procedures were performed and evidence gathered to support the accuracy of the audit conclusion. The audit findings and conclusion are based on a comparison of the conditions that existed as of the date of the audit against established criteria that were agreed upon with management. Further, the evidence was gathered in accordance with the *Internal Auditing Standards for the Government of Canada* and the *International Standards for the Professional Practice of Internal Auditing*. The audit conforms to the *Internal Auditing Standards for the Government of Canada*, as supported by the results of the quality assurance and improvement program.