Aboriginal Affairs and Northern Development Canada | Affaires autochtones et Développement du Nord Canada

Aboriginal Affairs and Northern Development Canada

Internal Audit Report Summary

Audit of Information Technology Security

Prepared by:

Audit and Assurance Services Branch

April 2015

TABLE OF CONTENTS

Acronyms

AANDC	Aboriginal Affairs and Northern Development Canada
DSO	Departmental Security Officer
DSP	Departmental Security Plan
IT	Information Technology
ITSC	Information Technology Security Coordinator
MITS	Operational Security Standard: Management of Information Technology Security

Background

As a federal government department, Aboriginal Affairs and Northern Development Canada (AANDC) is governed by the Treasury Board of Canada Secretariat's (TBS's) *Policy on Government Security*. Government security, in this overarching policy, refers to the assurance that information, assets and services are protected against compromise and individuals are protected against workplace violence. Elaborating on the information and information technology (IT) security aspect is the Treasury Board's *Operational Security Standard: Management of Information Technology Security* (MITS), which defines the baseline security requirements that federal departments must fulfill to ensure the security of information and information technology assets under their control.

According to MITS, IT security is defined as the "safeguards to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information" and, for the purposes of the standard, the "safeguards applied to the assets used to gather, process, receive, display, transmit, reconfigure, scan, store or destroy information electronically."

An effective security program combines tools and technologies to protect information and systems, and the coordination of a variety of stakeholders. At AANDC, two key roles with responsibility for IT security are the *Departmental Security Officer* (DSO), a Director of Security and Occupational Health and Safety, within the Human Resources and Workplace Services Branch, and the *IT Security Coordinator* (ITSC), a Manager of IT Security, within the Information Management Branch headed by the Chief Information Officer. The ITSC reports functionally to the DSO on security-related matters.

In 2011, Shared Services Canada was established and has assumed responsibility for the delivery, and related security, of some IT services – including email, data centres (with related hardware and systems software), telecommunication networks services and aspects of cyber security – formerly provided by AANDC.

The risks associated with the use of information technologies evolve as technologies continue to become more interconnected. AANDC's reliance on IT to process, store and transmit information in support of continuous program delivery combined with the Department's need to safeguard that information underscore the necessity of sound IT security controls and practices.

This audit was added to the Department's 2014-15 to 2016-17 Risk-Based Audit Plan at the request of the Deputy Minister of AANDC.

Audit Objective

The objective of the audit was to determine the adequacy and effectiveness of:

- the governance framework in place over IT security to protect the security of departmental information, and help to ensure compliance with the *Policy on Government Security* and the *Operational Security Standard: Management of Information Technology Security*; and,
- selected control frameworks in place to mitigate IT security risks.

Audit Scope

The scope included an examination of governance, risk management and key IT security controls designed to protect the security of information and information assets, and to help ensure compliance with the *Policy on Government Security* and the *Operational Security Standard: Management of Information Technology Security*.

In addition to the governance framework for all aspects of IT security, specific testing considered IT security controls over a selection of applications and network folders, as well as the controls implemented to protect desktops/laptops and removable media.

In particular, the audit work included:

- An examination of the IT security governance and risk management processes in place to manage the IT security program in the Department. This area focused on the IT security policy framework; IT security governance, roles and responsibilities; IT security planning and risk management; human resources planning; and compliance with federal government requirements.
- An examination of controls for a selection of areas where data is stored electronically within the Department, namely within applications and, if data is downloaded, on desktops/laptops or removable storage devices.

The period from July 2013 to December 2014 was included in scope, with most emphasis on more recent activities.

The audit excluded the assessment of business continuity planning and IT security activities under the responsibility of Shared Services Canada.

Audit fieldwork was mostly conducted at Headquarters but regional input was obtained with the help of a questionnaire sent to all regions.

Observed Strengths

The following strengths were identified during the audit:

- Governance - Key roles with responsibility for IT security, namely the DSO and the ITSC, have been clearly assigned and a departmental Security Committee facilitates the working relationship.
- Awareness - IT security is integrated into the security awareness program.

Findings

Based on a combination of the evidence gathered through the examination of documentation, analysis, interviews and process walk-throughs, each audit criterion was assessed. Where a significant difference between the audit criterion and the observed practice was found, the risk of the gap was evaluated and used to develop a conclusion and to document recommendations for improvement.

Observations were noted in the following areas during the audit:

- IT security awareness
- IT security incident management
- Policy framework
- Governance
- Planning and risk management
- Compliance
- Internal reporting
- Access to applications and data

Conclusion

The audit found that, while some of the elements that would be expected of an IT security program are in place, opportunities to improve the governance framework exist in the areas of IT security policy requirements, responsibility for IT security in the regions, risk management and proactive planning, on-going monitoring of compliance with federal government requirements. Opportunities also exist to improve some access controls relating to applications and data. The audit resulted in seven recommendations.

Statement of Conformance

The Audit of Information Technology Security conforms with the *Internal Auditing Standards for the Government of Canada*, as supported by the results of the quality assurance and improvement program.

Summary of Audit Criteria	
1.	Governance over IT Security
1.1	IT security policies aligned with the government's IT security policy framework have been developed and communicated across the Department.
1.2	Departmental oversight bodies for the management of IT security have been established.
1.3	A current IT security plan exists and is aligned with government-wide priorities.
1.4	An HR Plan for IT security staff exists and is aligned with priorities and plans.
1.5	A Departmental approach to managing IT security risks has been implemented.
1.6	Reporting on compliance and IT Security performance informs decision-making.
2.	IT Security Practices over Departmental Data
2.1	Controls are in place to restrict access to applications and network shares.
2.2	Controls are in place to restrict access to privileged accounts.
2.3	A security awareness program is in place.
2.4	A process exists to effectively manage IT security incidents that includes identification, detection, response and recovery procedures.