Crown-Indigenous Relations and Northern Affairs and Indigenous Services Canada

Final Internal Audit Report Summary

Audit of Information Technology Security

Prepared by:

Audit and Assurance Services Branch

March 2018

TABLE OF CONTENTS

Acronyms ii
Background 1
Audit Objective 2
Audit Scope 2
Observed Strengths 2
Findings 2
Conclusion 3
Statement of Conformance 3
Summary of Audit Criteria 3

Acronyms

CIO	Chief Information Officer
CSE	Communications Security Establishment
DSO	Departmental Security Officer
GC	Government of Canada
HQ	Headquarter
INAC	Indigenous and Northern Affairs Canada
IT	Information Technology
ITSG	Information Technology Security Guidance
MITS	Operational Security Standards: Management of Information Technology Security
SSC	Shared Services Canada
TB	Treasury Board
USB	Universal Serial Bus

Background

The Audit of Information Technology (IT) Security was included in the Indigenous and Northern Affairs Canada (INAC) 2017-2018 to 2019-2020 Risk-Based Audit Plan, approved by the Deputy Minister on March 13, 2017. The audit was identified as a high priority on the basis that IT security is complex and important to the operations of the Department, and very sensitive with potential for high impact of risk. IT Security is responsible for safeguarding personal and sensitive information and IT systems are part of the Department's critical infrastructure.

IT security refers to the safeguards that preserve the confidentiality, integrity, availability, intended use, and value of electronically stored, processed, or transmitted information. IT security also includes the safeguards that are applied to the assets used to gather, process, and store, or destroy information electronically. IT and its security are continuous processes as servers are active 24 hours a day, 365 days a year. There have been constant increases in the utilization of technological resources to process, store and transmit information in support of continuous program delivery. The Department's increased reliance on IT underscores the need to safeguard that information and the need for sound IT security controls and practices.

Recently, there have been numerous and ever-increasing instances of data and security breaches reported in Canada and affecting Canadians. Specifically affecting the Government of Canada, cyber-attacks have occurred targeting the National Research Council, Department of Finance, Department of National Defence, and the Treasury Board Secretariat among others. In addition to the cyber-attacks, other incidents of significance have occurred in numerous instances relating to the security and functionality of IT systems and services.

Currently, the Government of Canada (GC) is standardizing, consolidating, and re-engineering the way it does business internally. As part of the GC's Strategy for IT Modernization[1], Shared Services Canada (SSC) was established in 2011 to maintain and improve IT service delivery, generate savings, and implement government-wide solutions that are modern, reliable and secure. IT security governance has become inherently more complex, as it is now a shared responsibility between SSC and departments. SSC is responsible for INAC's perimeter of defence, network management, storage management, and server provisioning. INAC remains responsible for the management and security of desktops, database applications, and information.

As a federal government department, INAC is governed by the 2012 Treasury Board (TB) *Policy on Government Security*. Further to this policy, TB has issued a 2009 *Directive on Departmental Security Management*, which mandates that departments have a Departmental Security Policy. Elaborating on the information and IT security aspect is the 2004 TB *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 IT assets under their control. Further to these, Communications Security Establishment (CSE) issued the *Information Technology Security Guidance 33* (ITSG-33) in 2012 related to IT security risk management. It is important to note that the use of MITS is currently being phased out, while ITSG-33 is being more widely implemented.

An effective security program combines tools and technologies with user training and awareness to protect information and systems, and the coordination by a variety of

[1] *Government of Canada Information Technology Strategic Plan 2016-2020*

stakeholders. This type of program is important considering the number of applications hosted by INAC. At INAC, two key roles with responsibility for IT security are the Chief Information Officer (CIO), in charge of the Information Management Branch of the Chief Finances, Results and Delivery Officer Sector, who is the lead on IT security supported by an IT Security Coordinator as defined in MITS, and the Departmental Security Officer (DSO), a role of the Director of Security and Accommodation, within the Human Resources and Workplace Services Branch.

The audit was completed prior to the dissolution of INAC and the creation of Crown-Indigenous Relations and Northern Affairs (CIRNA) and Indigenous Services Canada (ISC). The findings and recommendations of this audit apply to both Departments.

Audit Objective

The objective of the audit was to assess the Department's compliance with the relevant IT security components of the TB Policy on Government Security and the MITS; and the relevant control frameworks in place to mitigate IT security risks.

Audit Scope

The scope of the audit included an assessment of the adequacy and effectiveness of the management, operational and technical controls in place over IT security to protect departmental information and IT assets. The audit included liaison and communications between SSC and INAC related to cyber security processes, but excluded a direct review of SSC operations as this was not a joint audit with SSC. Therefore, this audit provides assurance on INAC IT security activities. However, it is expected that INAC has to work in collaboration with SSC to implement the recommendations included in this report.

The audit team conducted fieldwork at INAC headquarters, two regional offices (Quebec and Ontario) and one additional regional office was contacted through teleconferencing (British Columbia). The audit also included the testing of key INAC applications.

Observed Strengths

The following strengths were identified during the audit:

- Secret documents are managed effectively;
- Tools are in place to help prevent malware from infecting workstations and the Department has implemented filtering of cloud storage services to help prevent unauthorized storage of documents in the cloud; and
- INAC has formalized the Regional Security Officer and Regional Informatics Manager roles related to IT Security.

Findings

Based on a combination of evidence gathered through the examination of documentation, analysis and interviews, each audit criterion was assessed by the audit team and a conclusion for each audit criterion was determined. Where differences between the audit criteria and the observed practice were found, the risk of the gap was evaluated and used to develop a conclusion and to document recommendations for improvement initiatives.

Observations were noted in the following areas during the audit:

- Security Monitoring Management;
- Management of Sensitive Information;
- User Access Management;
- Development and Implementation of Secure IT Applications; and
- IT Continuity.

Conclusion

The audit concluded that while key management controls are in place related to IT security, opportunities exist in the areas of: Security Monitoring Management, Management of Sensitive Information; User Access Management, Development and Implementation of Secure IT Applications; and IT Continuity. The audit resulted in five recommendations.

Statement of Conformance

The audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing*, as supported by the results of the quality assurance and improvement program.

Summary of Audit Criteria

To ensure an appropriate level of assurance to meet the audit objectives, the following audit criteria were developed to address the objectives.

Audit Criteria	
1. There are effective managerial IT security controls in place to meet policy requirements and mitigate risks.	
1.1	Roles and responsibilities related to IT security between Information Management Branch, regions and SSC are clearly defined and communicated.
1.2	An IT Security plan has been developed in alignment with the IT plan to address IT security risks and compliance requirements (CSE Top 10, Security Policy Implementation Notices).
1.3	The department ensures that appropriate processes are in place to comply with IT security policy instruments.
2. There are effective IT security operational and technical controls in place to meet policy requirements and mitigate risks.	
2.1	There is an effective process to identify and recover from incidents in a timely manner.
2.2	IT systems and safeguards are effective in managing classified information.
2.3	Regional offices operations are aligned with HQ's requirements.
2.4	There are effective safeguards in place to protect INAC's sensitive electronic information from cyber-attacks.
2.5	There is an effective process to recover from IT disasters in a timely manner.