Audit of Information Technology (IT) Security

Notice to readers: *This report contains confidential information, or information related to security, which has been redacted in accordance with the Access to Information Act.*

Corporate Internal Audit Division
Natural Sciences and Engineering Research Council of Canada /
Social Sciences and Humanities Research Council of Canada

Approved by the Presidents on July 23, 2021

Aussi disponible en français sous le titre : Audit de la sécurité des technologies de l'information

For more information, contact

Natural Sciences and Engineering Research Council of Canada
350 Albert Street
Ottawa, Ontario K1A 1H5
www.nserc-crsng.gc.ca

Cat. No. NS3-58/2021E-PDF
ISBN 978-0-660-40626-8

TABLE OF CONTENTS

BACKGROUND

The Natural Sciences and Engineering Research Council (NSERC) and the Social Sciences and Humanities Research Council (SSHRC) (the 'Agencies') are departmental agencies of the Government of Canada created in 1977 and 1978, respectively. The Agencies are funded directly by Parliament to support scholarly endeavors in Canada's post-secondary institutions and report to Parliament through the Minister of Innovation, Science and Industry. The Agencies share a Common Administrative Services Directorate (CASD), which is responsible for shared services of Human Resources, Finance and Awards Administration, and Information and Innovation Services (IIS).

WHY IS IT IMPORTANT

The relentless pace of digital business and ongoing transition to cloud are creating new challenges for both private and public sector entities. Traditional IT security approaches need to evolve with the changing landscape, and acting on these developments, government entities can improve resilience, better support business objectives, and reduce the risk of IT security compromise.

OBJECTIVE AND SCOPE

The objective of this audit was to assess the effectiveness of specific aspects of the Agencies' IT Security management framework, including the effectiveness of technical and operational safeguards in the areas of IT security policy, IT security awareness, IT security risk management, network vulnerability management, and system development, including the use of data.

The scope of the audit focused primarily on the areas of high risk identified in the 2019 Preliminary Survey of IT Security:

- IT security policy
- IT security user awareness and training
- IT security risk management
- Threat and vulnerability management
- System development and the use of data

Controls that reside at any IT service providers outside of CASD were out of scope.

AUDIT METHODOLOGY

During the planning phase the audit team conducted a risk assessment and a validation of information resulting from the 2019 Preliminary Survey of IT Security. Based on this assessment, the team focused their analysis on the following elements: IT security policies, roles and responsibilities, user awareness and training, risk management, IT threat and vulnerability management, and data used in system development.

The audit was conducted jointly by the Corporate Internal Audit Division (CIAD) team and an external assurance provider. The methodology for the audit included review of documentation, interviews with management and staff, and testing of key controls.

The Treasury Board's *Policy on Internal Audit* sets out the responsibilities of the NSERC/SSHRC deputy heads. In accordance with the Treasury Board's *Policy on Internal Audit*, the audit was carried out in accordance with the Institute of Internal Auditors' International Professional Practices Framework.

WHAT WAS FOUND

During the audit, a number of **strengths** associated with the Agencies' IT security program were identified by the audit team, as follows:

- The Agencies developed a comprehensive Departmental Security Plan through a risk-based approach, which included action plans to increase the Agencies' IT security posture.
- Several mechanisms and tools are in place to identify IT security events on the infrastructure layer, and a vulnerability management process has been developed.
- The Agencies have designed and implemented mandatory IT security training for all new employees; and,
- The Agencies have formally assessed their IT environment against the Canadian Centre for Cyber Security's Top 10 IT Security Actions[1]. This included formally documented responses to each recommended security action, with action plans to address any gaps.

During the audit some areas were also noted where improvements to IT security can be made, as follows:

- [redacted for security reasons]
- [redacted for security reasons]
- The processes for ensuring changes to IT systems are appropriately tracked, and then assessed from an IT security standpoint have not been formalized or implemented. Without a formally documented security assessment process, there's an increase risk that systems will be developed and used that do not meet the security requirements.
- [redacted for security reasons]
- A process to track and manage IT threats and vulnerabilities is not in place at the application layer to proactively identify and manage IT security vulnerabilities. Without actively managing IT threats and vulnerabilities, there's an increased risk that vulnerabilities are not being addressed in a prioritized or timely manner.

CONCLUSION

Management has established some level of IT security controls in each of the IT security areas that were assessed during the audit; however, as the Agencies continue to become more digital, including migration to more modern technologies in the cloud and otherwise, there is room to improve how IT risk management activities are carried out. [redacted for security reasons]

[1] https://cyber.gc.ca/en/top-10-it-security-actions

MANAGEMENT RESPONSE AND ACTION PLAN

ITEM	RECOMMENDATION	MANAGEMENT RESPONSE AND ACTION PLAN	TARGET DATE
1.	[redacted for security reasons]	[redacted for security reasons]	[redacted for security reasons]
2.	[redacted for security reasons]	[redacted for security reasons]	[redacted for security reasons]
3.	It is recommended that the CIO formalize their security assessment and authorization (SA&A) processes and approach, and ensure that it is appropriately embedded within the IT system development and maintenance lifecycle. This should include formal tracking and monitoring of security assessment and authorization activities to be able to report and ensure that recommended safeguards are implemented in a timely manner.	The IT Security Coordinator will formalize, document and communicate the framework for the Security Assessment & Authorization process which will include, maintenance and life cycle. The Chief Information Officer in collaboration with the Chief Security Officer will ensure the framework is applied to all systems lifecycle.	March 2022
4.	[redacted for security reasons]	[redacted for security reasons]	[redacted for security reasons]
5.	It is recommended that the CIO further develop this program to include the logging, prioritization and tracking of IT threats and vulnerabilities. Furthermore, a risk-based approach should be applied when conducting penetration testing across the application portfolio.	The IT Security Coordinator will ensure the current process is formalized, documented, in order to log and track IT threats and vulnerabilities. This process will capture a risk-based strategy when conducting penetration testing across the application portfolio.	March 2022