Internal Audit of the Personnel Security Screening Process - Internal Audit Report

Presented by Internal Audit Directorate

September 26, 2023

Table of Contents

Executive Summary

The Audit of Personnel Security Screening Process was authorized as part of the Department of Finance Canada's (the Department) 2022-2023 Risk-based Audit Plan, which was approved by the Deputy Minister on June 29, 2022.

What we examined

The objective of this audit was to provide reasonable assurance that the Department's personnel security screening process' internal controls are effective and efficient, and that the process is compliant with applicable policies.

Why it is important

Employees at the Department require access to sensitive information to perform their work in support of providing strategic analysis and advice to the Minister of Finance. Effective personnel security screening can provide some level of reassurance that employees can be trusted to safeguard government information, assets and facilities, and to reliably fulfill their duties.

What we found

Up to the granting of a security clearance, the Department has effective controls in place for the personnel security screening process. However, significant control weaknesses were identified regarding the close-out of the process.

Areas of improvement were identified with respect to the overall efficiency of the personnel security screening process. Given the context of the remote work period, processing delays by other involved organizations, and the current resources assigned to the process, these findings are not unexpected.

Also, the Department's personnel security screening process is not compliant with some applicable Treasury Board policy suite requirements. The Department does not currently have a Departmental Security Plan and a security delegation instrument.

The following table summarizes the overall findings and the associated risk to the Department:

Table 1

Overall Findings and Associated Risks

Overall Findings	Risk	Policy Requirement (Y/N)
The Department currently has no Departmental Security Plan.	High	Y
The Department currently has no security delegation instrument to document decision-making authorities.	Medium	Y

Overall Findings	Risk	Policy Requirement (Y/N)
No tracking is currently being done to ensure that all employees have attended the Department's mandatory security briefing.	Medium	Y
Security certificates (TBS form 330-47) were generally not signed in a timely manner or were not signed at all.	Medium	Y
Notifications to the Canadian Security Intelligence Service (CSIS) regarding the status of security clearances issued were generally not sent in a timely manner or were not sent at all.	Medium	Y
No exit security debriefs are being conducted for employees leaving the Department.	Medium	Y
The security screening process is currently paper-based, which resulted in a large backlog of files waiting to be processed during the remote-work period caused by the COVID-19 pandemic.	Medium	N
Transfer-in security files of employees coming from other departments were either never received by the Department, received significantly after the date requested, or were incomplete. However, the audit team was able to confirm that the employees did have a valid security clearance.	Medium	N

Overall Findings	Risk	Policy Requirement (Y/N)
Personnel security officers have checklists to ensure completeness of files but do not use the checklists effectively.	Medium	N
There is limited communications to managers and employees reminding them of their security-related responsibilities.	Medium	N
The Departmental Security Policy was last revised in 2011 and contains outdated information.	Medium	N
A significant amount of time is spent on manual data entry by personnel security officers.	Low	N
An agreement is in place with CSIS to prioritize security assessments for candidates hired through the University Recruitment and Advanced Policy Analyst Program processes. This agreement is not formally documented.	Low	N
The Department's main forum for discussing sensitive security-related issues has stopped meeting. Meetings between the Department's key security officials currently take place informally.	Low	N

Marie-Josée Yelle

Acting Chief Audit Executive

Background

Within the Department of Finance Canada (the Department), employees are required to access protected and/or classified information to perform their work in support of providing strategic analysis and advice to the Minister of Finance. To reduce the risk that protected and/or classified information is inappropriately accessed, used or shared, the Government of Canada has established security controls and policies, including policies related to personnel security screening.

Personnel security screening involves the collection of personal information from individuals, with their informed consent, and information from law enforcement, intelligence sources, and other sources and methods to assess an individual's reliability and loyalty to Canada. Effective personnel security screening can provide some level of reassurance that employees can be trusted to safeguard government information, assets and facilities, and to reliably fulfill their duties.

The management of personnel security screening is primarily governed by the Treasury Board's (TB) Policy on Government Security, Directive on Security Management, and Standard on Security Screening (Standard). The objective of the Standard is to ensure that security screening in the Government of Canada is conducted in a way that is effective, efficient, rigorous, consistent and fair to provide reasonable assurance that individuals can be trusted to safeguard government information and assets and can reliably conduct their work duties, as well as to enable transferability of security screening between departments and agencies.

The Standard also defines the following security status and clearances:

- Reliability status is the minimum standard of security screening for positions requiring unsupervised access to Government of Canada

protected information, assets, facilities or information technology systems.

- Secret clearance is the standard of security screening for all positions requiring access to Government of Canada information, assets, facilities or information technology systems classified as Secret.
- Top Secret clearance screening is conducted for positions requiring access to top secret Government of Canada information, assets, facilities or IT systems.

Given the sensitive nature of information within the Department, all its employees are required to have a minimum of a Secret clearance.

Within the Department, the Assistant Deputy Minister, Corporate Services Branch (CSB), has been designated as the Department's Chief Security Officer. The Security Services Division (SSD), within the Human Resources and Security Directorate of CSB, is responsible for the personnel security screening process. In addition, SSD is responsible for security incident management, emergency preparedness, ministerial security, physical security, security event management, business continuity management, and security in contracts and other arrangements. At the time of the audit, the SSD team consisted of five (5) full-time employees (FTEs), with one (1) FTE dedicated full-time to personnel security screenings.

The following government departments also play a role in the security screening process:

- The Canadian Security Intelligence Service's (CSIS) Government Security Screening program investigates and provides security assessments for persons requiring Secret or Top Secret level security clearances as part of their employment.
- The Royal Canadian Mounted Police (RCMP) is responsible for performing the criminal record check portion of the personnel security screening.

Audit Objective, Scope, Criteria, and Approach

Audit Objective and Scope

Audit Objective:

- The objective of this audit engagement was to provide reasonable assurance that the Department of Finance Canada's (the Department) personnel security screening process' internal controls are effective and efficient, and that the process is compliant with applicable policies.

Audit Scope:

- The audit scope included an assessment of the key controls pertaining to the personnel security screening process, as well as a review of personnel security screening transactions (assignment, renewal, and revocation of security clearances) between April 1, 2019, and September 30, 2022.
- The scope did not include:
  - Processes for site access screenings, used for individuals external to government who do not require access to sensitive information but require access to restricted or controlled government facilities.
  - Parts of the personnel security screening process that are owned by other federal organizations (for example, the Canadian Security Intelligence Service and the Royal Canadian Mounted Police).
  - Other preventative, detective or corrective controls that are part of an Insider Risk Program. [1]
  - The efficiency and effectiveness of the Department's Human Resources staffing processes.

- An assessment of compliance against policy suite requirements not related to personnel security screening.

Audit Criteria

Criterion 1: The Department's personnel security screening process' internal controls are effective; and are in compliance with the Treasury Board (TB) Policy on Government Security, Directive on Security Management, and Standard on Security Screening.

Criterion 2: Personnel security screenings are processed effectively and efficiently.

Audit Approach

In conducting this audit we:

- Reviewed relevant documentation such as legislation, policies and guidance, administrative agreements, and departmental guidance.
- Interviewed personnel from the Corporate Services Branch.
- Identified key controls and developed process maps.
- Tested a judgmental sample of 46 personnel security files from the period examined to assess compliance with relevant legislation, policies, and guidance.
- Performed benchmarking against other federal departments and agencies.

Overall Opinion and Statement of Conformance

Overall Opinion

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.

The findings and conclusion are only applicable to the entities examined and for the scope and time period covered by the audit.

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 Findings

Key Findings – Note

Given the current resources within the Security Services Division assigned to the personnel security screening process, the internal audit team has issued a formal recommendation for findings non-compliant with policy. Where a formal recommendation has been issued, management has

developed a Management Action Plan (MAP). The Internal Audit Directorate (IAD) will follow-up on these MAPs to ensure that they have been implemented.

The IAD will not follow-up on areas of consideration on the overall efficiency and effectiveness of the process as it is management's prerogative to risk-manage these areas.

Key Findings – Criterion 1

We expected to find that the Department of Finance Canada's (the Department) personnel security screening process' internal controls are effective; and are in compliance with the Treasury Board (TB) Policy on government Security, Directive on Security Management, and Standard on Security Screening.

The internal audit team found that the three (3) major verifications that take place during the security screening (criminal record check, credit check and the Canadian Security Intelligence Service (CSIS) security assessment) were conducted 100% of the time in the files that were reviewed. The internal audit team also noted that when adverse information [2] was uncovered or information was incomplete, that there are processes in place to conduct security interviews when necessary or to obtain missing information. The following table outlines findings, as well as recommendations for management's action:

Table 2

Criterion 1 - Findings and Recommendation

Findings	Recommendations	Risk

Findings	Recommendations	Risk
The Deputy Minister (DM) is responsible for approving a three-year Departmental Security Plan (DSP) that is reviewed annually, sets out strategies for meeting departmental security requirements reflective of and contributing to government-wide security priorities, and addresses required security controls. The Department previously had a 2019-21 DSP that was approved by the DM in January 2020. At the time of the examination phase work completed by the audit team, there was no current DSP in place. [This information has been severed.] The Corporate Services Branch has hired a consultant to develop a DSP and is aiming to have one drafted by Spring 2023. The Chief Security Officer (the Assistant Deputy Minister, Corporate Services Branch) is required to report annually to the DM on the progress made against the priorities defined in the DSP. Given that there is no current DSP in place, there has	The Chief Security Officer should develop a three-year Departmental Security Plan (DSP), have it approved by the Deputy Minister (DM), and report annually to the DM on the progress made against its priorities.	High

Findings	Recommendations	Risk
been no annual reporting to the DM. Reviewing and reporting annually on the DSP allows departments to demonstrate that appropriate governance is in place to provide a comprehensive understanding of security management, security priorities, and risk mitigations throughout the organization and provides the opportunity to course-correct or re-prioritize activities as needed.		
The Chief Security Officer has responsibilities to define and document security related roles, responsibilities and decision-making authorities to ensure consistency, efficiency and maintaining compliance with relevant legislation. The Department currently has no security delegation instrument in place.	The Chief Security Officer should create a security delegation instrument and have it approved by the Deputy Minister.	Medium

Findings	Recommendations	Risk
Employees are required to attend a mandatory security briefing when they join the Department and then acknowledge their responsibilities by signing a security certificate (Treasury Board Secretariat form 330-47). There is currently no tracking being done to ensure that all employees at the Department have attended the mandatory briefing. The internal audit team noted from the files reviewed that, generally, security certificates were not signed by employees, or not signed on a timely basis. This increases the risk that employees may not be aware of their responsibilities towards the protection of information with regards to their security clearance. [This information has been severed.]	The Chief Security Officer should improve the controls in place to ensure that all employees receive the mandatory security briefing and acknowledge their responsibilities by signing their security certificate.	Medium

Findings	Recommendations	Risk
The Department is responsible for notifying the Canadian Security Intelligence Service (CSIS) when new security clearances are granted (CSIS form 4195) or when there has been a change in security clearance, such as a transfer, a downgrade, an upgrade or a re-activation (CSIS form 4160). The internal audit team noted, from the files reviewed, that notifications to CSIS were not sent in a timely manner or were not sent at all. [This information has been severed.]	The Chief Security Officer should improve the controls in place to ensure that personnel security officers are notifying CSIS in a timely manner when a clearance is granted (CSIS form 4195) or an employee security file is transferred between departments, downgraded, upgraded or re-activated (CSIS form 4160).	Medium

Findings	Recommendations	Risk
The Department is responsible for providing a formal debriefing to employees who are leaving the Department to remind them of their continuing responsibilities to maintain the confidentiality of the sensitive information to which they previously had access to. The internal audit team noted that no exit security debriefs were currently being conducted. There is currently a risk that employees can leave the department and not be aware of their continued responsibilities for the protection of information for which they had access to at the Department and may divulge sensitive information.	The Chief Security Officer should ensure that a process is put in place to debrief employees of their continued security responsibilities prior to leaving the Department.	Medium

Key Findings – Criterion 2

We expected to find that personnel security screenings are processed effectively and efficiently.

Areas of improvement were identified with respect to the efficiency and effectiveness of the security screening process as a whole. The following table outlines the internal audit team's findings as well as some

suggestions for management's consideration.

Table 3

Criterion 2 - Findings and Areas of Considerations

Findings	Areas of Consideration	Risk

Findings	Areas of Consideration	Risk
The Department's security screening process is paper based. Following the onset of the COVID-19 pandemic and the remote work orders, the Security Services Division (SSD) stopped processing certain types of transactions as they were working from home and did not have access to printers, thus creating a large backlog of files that needed to be processed in person. It was also observed during file reviews that printing the personnel security files was very time consuming, given that several of the reports generated during the screening process were already in digital format. From outreach done to other government departments, the internal audit team noted that several departments have switched to digital files and are accepting digital signatures on security screening forms in order to increase efficiency in the new hybrid work environment. This also increased efficiency in the ability to transfer files to other departments once an employee had transferred to a different department.	The Chief Security Officer may consider working towards the digitization of all personnel security files and use digital signatures where possible. The Chief Security Officer should ensure that the backlog of transfer-in and transfer-out files to other departments is cleared on a regular basis.	Medium

Findings	Areas of Consideration	Risk
Transfer-in security files of employees coming from other departments were either never received by the Department, received significantly after the date requested, or were incomplete. However, the audit team was able to confirm that the employees did have a valid security clearance. The internal audit team noted that some departments redo the reliability status for all transfer-in employees. Ensuring that the employee has no adverse results on a criminal record check or credit check reduces the risk to the Department that the employee may divulge sensitive information in exchange for money.	The Chief Security Officer may consider redoing the reliability status of federal employees transferring in from other departments using a risk-based approach.	Medium

Findings	Areas of Consideration	Risk
Checklists are used by personnel security officers to document that all required steps in the process have been completed. Checklists can be an effective tool in ensuring that all steps of a process have been completed. From a review of personnel security files, the internal audit team noted that the checklists were often not signed, dated, or they noted that certain steps of the process had been completed when in fact they had not. The internal audit team also noted that the checklists were generally completed by a junior member of the Security Services Division (SSD).	The Chief Security Officer may consider incorporating a monitoring process conducted by a more senior employee to review completeness of files.	Medium

Findings	Areas of Consideration	Risk
Managers have responsibilities to ensure that their employees have been informed of their security responsibilities. Managers also have responsibilities for monitoring their employees for significant changes in behaviour and reporting these changes to SSD. Employees have responsibilities to notify SSD of changes in personal circumstance, persistent or unusual contact, or any unusual behaviours of other individuals. The internal audit team found that there is limited communications to managers and employees reminding them of their responsibilities regarding personnel security.	The Chief Security Officer may consider increasing security awareness throughout the Department, including roles and responsibilities.	Medium
The Departmental Security Policy was last revised in 2011 and contains outdated information. Not having an up-to-date policy increases the risk that roles, responsibilities and overall security-related objectives are not clearly defined and understood.	The Chief Security Officer may consider reviewing and updating the Department's Security Policy.	Medium

Findings	Areas of Consideration	Risk
There is a significant amount of time spent by personnel security officers doing manual data entry. Not only is this time consuming, but manual data entry increases the risk of human input errors. From outreach to other government departments, it was noted that several departments have already implemented, or are looking to implement, digital form submission portals. This would reduce the need for manual data entry, the submission of incomplete forms, and the subsequent back and forth between the personnel security officer and the applicant.	The Chief Security Officer may consider exploring options to implement a new automated security screening system to reduce the need for manual data entry from security screening forms.	Low

Findings	Areas of Consideration	Risk
Significant delays in the screening process are caused by a backlog at CSIS in conducting security assessments. The Department has a special agreement with CSIS to give priority to the security assessment for candidates hired through the University Recruitment (UR) program and the Advanced Policy Analyst Program (APAP). This agreement is informal and is not documented. Given high turnover at CSIS, there is a risk that this agreement may not carry forward if certain employees with CSIS leave their positions.	The Chief Security Officer may consider formalizing a written agreement with CSIS.	Low

Findings	Areas of Consideration	Risk
Formalizing governance structures and documenting decisions assists in holding individuals accountable for decisions and in ensuring appropriate follow-up action can be taken. The Department of Finance Security Coordinating Committee (FINSCC), the Department's main forum for discussing sensitive security-related issues, has stopped meeting. Meetings between key security officials are now taking place informally. Given that no records of these meetings are kept, the internal audit team was unable to conclude on the effectiveness of oversight.	The Chief Security Officer may consider reformalizing the governance of the Department's security program.	Low

Overall Conclusion

Up to the granting of a security clearance, the Department of Finance Canada (the Department) has effective controls in place for the personnel security screening process. However, significant control weaknesses were identified regarding the close-out of the process.

Areas of improvement were identified with respect to the overall efficiency of the personnel security screening process. Given the context of the remote work period, processing delays by other involved organizations,

and the current resources assigned to the process, these findings are not unexpected.

Also, the Department's personnel security screening process is not compliant with some applicable Treasury Board policy suite requirements. The Department does not currently have a Departmental Security Plan and a security delegation instrument.

Management Response and Action Plans

Overall Management Response:

Management agrees with the findings of the Audit of the Personnel Security Screening Process. The Chief Security Officer will work with the Security Services Division to ensure that audit recommendations are addressed through corrective actions, as described below.

Table 4

Management Response and Action Plans

Recommendation	Management Response	Action Plan	Lead	Targ

Recommendation	Management Response	Action Plan	Lead	Targ
1. The Chief Security Officer should develop a three-year Departmental Security Plan (DSP), have it approved by the Deputy Minister, and report annually to the Deputy Minister on the progress made against the priorities defined in the DSP.	Management agrees with the recommendation.	The Chief Security Officer (CSO) will develop a three-year Departmental Security Plan (DSP) and submit it for Deputy Minister approval. The CSO will also report annually to the Deputy Minister on progress made against the priorities defined in the approved DSP.	Chief Security Officer, Assistant Deputy Minister – Corporate Services Branch	Three Depa Secu Octol 2023 First progr repor Depu Minis Marc 2025

Recommendation	Management Response	Action Plan	Lead	Targ
2. The Chief Security Officer should create a security delegation instrument and have it approved by the Deputy Minister.	Management agrees with the recommendation.	The Chief Security Officer will develop a security delegation instrument and present it to the Deputy Minister, for approval.	Chief Security Officer, Assistant Deputy Minister – Corporate Services Branch	Septe 30, 2(

Recommendation	Management Response	Action Plan	Lead	Targ
3. The Chief Security Officer should improve the controls in place to ensure that all employees receive the mandatory security briefing and acknowledge their responsibilities by signing their security certificate.	Management agrees with the recommendation.	The Director, Security Services Division (SSD), will integrate enhanced controls in the departmental onboarding process to ensure that all employees have received the mandatory security briefing and acknowledged their responsibilities by signing their security certificate. The Director, SSD, will provide an annual report of results achieved to the Deputy Chief Security Officer.	Director, Security Services Division	Marc 2024

Recommendation	Management Response	Action Plan	Lead	Targ
4. The Chief Security Officer should ensure that a process is put in place to debrief employees of their continued security responsibilities prior to leaving the Department.	Management agrees with the recommendation.	The Director, Security Services Division (SSD), will develop and implement a process to ensure that employees receive a briefing on their continued security responsibilities prior to leaving the Department. The Director, SSD, will provide an annual report of results achieved to the Deputy Chief Security Officer.	Director, Security Services Division	Marc 2024

Recommendation	Management Response	Action Plan	Lead	Targ
5. The Chief Security Officer should improve the controls in place to ensure that personnel security officers are notifying the Canadian Security Intelligence Service (CSIS) in a timely manner when a clearance is granted (CSIS form 4195) or an employee security file is transferred between departments (CSIS form 4160).	Management agrees with the recommendation.	The Director, Security Services Division (SSD), will adapt existing operating procedures and improve controls in place to ensure that personnel security officers notify CSIS in a timely manner when clearance is granted or when an employee security file is transferred between departments. The Director, SSD, will provide an annual report of results	Director, Security Services Division	Marc 2024

Recommendation	Management Response	Action Plan	Lead	Targ
		achieved to the Deputy Chief Security Officer.		

Appendix A – Compliance Testing Results

Table A1

Compliance Testing Results - New Clearances and Renewals

Test Criteria – New clearances and Renewals	Transactions tested	Files with issues	Additional Information
Applicant completed and signed security screening form providing consent to conduct the security screening (TBS form 330-23)	31	3	• One (1) file did not have the form on file. This clearance was completed during the early onset of the remote work orders. • Two (2) files had typed signatures (not an Entrust digital signature or wet signature) and were not dated.

Test Criteria – New clearances and Renewals	Transactions tested	Files with issues	Additional Information
Applicant completed and signed 330-60	31	4	• One (1) file did not have the form on file. This clearance was completed during the early onset of the remote work orders. • Three (3) files had typed signatures (not an Entrust digital signature or wet signature) and were not dated.
Criminal record check completed	31	0	• N/A – no control weaknesses found
Credit check completed	31	0	• N/A – no control weaknesses found
When adverse information is uncovered, further investigation is completed	1	0	• N/A – no control weaknesses found

Test Criteria – New clearances and Renewals	Transactions tested	Files with issues	Additional Information
Personnel Security Officer granted reliability status	31	2	• One (1) file did not have the form on file. This clearance was completed during the early onset of the remote work orders. • One (1) file had no signature from the personnel security officer.
CSIS security assessment completed	31	0	• N/A – no control weaknesses found
Personnel Security Officer granted security clearance	31	2	• One (1) file did not have the form on file. This clearance was completed during the early onset of the remote work orders. • One (1) file had no signature from the personnel security officer.

Test Criteria – New clearances and Renewals	Transactions tested	Files with issues	Additional Information
CSIS was notified of decision to grant a security clearance (CSIS form 4195)	31	2	• Two (2) files contained no form 4195 notifying CSIS of a security clearance granted. • Several files reviewed had the form 4195 sent months to years after the security clearance was granted. This was a result of personnel security officers working remotely and not coming into the office to print forms, thus creating a large backlog of forms following the return to office.

Test Criteria – New clearances and Renewals	Transactions tested	Files with issues	Additional Information
Employee received a mandatory security briefing	31	Unable to assess	• The internal audit team was unable to assess given that there is currently no master tracking being done to ensure that all employees at the Department have attended the mandatory briefing.
Employee acknowledged their responsibilities by signing a security certificate (TBS form 330-47)	31	19	• Personnel security officers put this practice on hold during much of the remote work period, thus creating a large backlog of certificates to be signed following the return to office. • Seven (7) certificates were signed after the internal audit team's initial file request (February 8, 2023).

Table A2

Compliance Testing Results - Transfer-In Employees

Test Criteria – Transfer-In Employees	Transactions tested	Files with Issues	Additional Information
The Department received an initial security clearance confirmation from the originating department	12	1	• One (1) personnel security file did not contain evidence of the original clearance confirmation request or response from the other department. However, a copy of the security file was received by the Department and the applicant had a valid security clearance, therefore the risk is low.
The Department requested the transfer of the personnel security file	12	0	• N/A – no control weaknesses found

Test Criteria – Transfer-In Employees	Transactions tested	Files with Issues	Additional Information
The file was received	12	2	• Two (2) files requested were not yet received by the Department. One file was requested on March 3, 2020 and the other file was requested on July 6, 2022.
The file transferred was complete (included credit check, criminal record check, and CSIS assessment)	10	5	• Two (2) files reviewed did not include the results of the criminal record check. • Three (3) files reviewed did not include the results of the credit check.
CSIS was notified of employee's transfer (CSIS form 4160)	10	2	• Two (2) files reviewed did not contain form 4160 to notify CSIS of the security clearance transfer.

Test Criteria – Transfer-In Employees	Transactions tested	Files with Issues	Additional Information
Employee received a mandatory security briefing	12	Unable to assess	• There is currently no master tracking being done to ensure that all employees at the Department have attended the mandatory briefing. The internal audit team was unable to assess.
Employee acknowledged their responsibilities by signing a security certificate (TBS form 330-47)	12	12	• Zero (0) of the files reviewed for a transfer-in employee contained a signed security certificate.

Table A3

Compliance Testing Results - Transfer-Out Employees

Test Criteria – Transfer-Out Employees	Transactions tested	Files with Issues	Additional Information
CSIS was notified of employee's transfer (CSIS form 4160)	3	0	• N/A – no control weaknesses found

Test Criteria – Transfer-Out Employees	Transactions tested	Files with Issues	Additional Information
The Department transferred the personnel security file to the requesting Department	3	0	• N/A – no control weaknesses found

Appendix B – Sampling Strategy

The internal audit team identified a population of 510 new and renewal security clearances, a population of 484 transfer-in security clearances and a population of 264 transfer-out security clearances for the period of April 1, 2019 to September 30, 2022. [3]

- For the new and renewal security clearances, out of the 510 security clearance files, 30 were selected using a judgemental random sampling method. [4]
- For the transfer-in security clearances, out of the 484 security clearance files, 12 were selected using a judgemental random sampling method.
- For the transfer-out security clearances, out of the 264 security clearance files, 3 were selected using a judgemental random sampling method.

The sample and population distribution is as follows:

Table B1

Sampling Strategy

Stratification [5]	Sample Count				Populati		
	April 1, 2019 - March 15, 2020	March 16, 2020 - May 3, 2020	May 4, 2020 - August 31, 2020	September 1, 2020 - September 30, 2022	April 1, 2019 - March 15, 2020	March 16, 2020 - May 3, 2020	M 20 Au 31 20
New and renewal security clearances	6	3	6	16	195	20	
Transfer-in security clearances	4	8			138		
Transfer-out security clearances	3						26
Total	**45**						**12**

Appendix C – Key Information Reviewed

Key Information Reviewed

The following is a non-exhaustive list of key information reviewed by the internal audit team:

Legislation, policies and guidelines:

- Treasury Board (TB) Policy on Government Security

- TB Directive on Security Management
- TB Standard on Security Screening

Documents specific to Department of Finance Canada:

- Departmental Security Policy (2011)
- 2019-21 Departmental Security Plan
- Department of Finance Management Accountability Framework Departmental Reports (2020-21 and 2021-22)
- Department of Finance Canada's Threat Risk Assessments
- Departmental of Finance governance committee documentation, such as Terms of Reference and records of decision
- Security Services Division internal process documentation

Other Documents:

- Canadian Security Intelligence Service's Insider Risk Program Reference Guide

Appendix D – Risk Ranking Methodology

The risks assigned to the findings were based on the Internal Audit Directorate's own assessment of the risks. The following table defines the criteria used in assigning risk/priority:

Table D1

Risk Ranking Methodology

High-Risk Zone	Risks that significantly exceed the risk acceptance threshold and need extensive management and, in some cases, urgent action.
Medium-Risk Zone	Risks that exceed the risk acceptance threshold and require proactive management.

Low-Risk Zone	Risks that are below the risk acceptance threshold and do not generally require active management.

Footnotes

1 An Insider Risk Program is designed to deter, detect and respond to workforce behaviours and activities that can compromise the safety and security of an organization's sensitive assets. A sound and comprehensive Insider Risk Program is comprised of several components, one of which includes personnel security screening.

2 Adverse information: information about an applicant that may hamper or expose an organization to risks (i.e. a criminal record, poor credit score, etc.). Adverse information can, but may not be, sufficient grounds to deny or revoke a security clearance. When uncovered, such information is to be used as the basis for further investigation.

3 Completeness of the population was verified by comparing the Security Services Division (SSD) Access database population against the Peoplesoft population shared by Human Resources in Corporate Services Branch. The population used for sampling was extracted from the SSD Access database.

4 A judgmental random sample was selected due to the limited resources in SSD and to reduce the impact on personnel security screening staff. The number of samples selected were based on the judgement of the internal audit team while the individual sample files were randomly selected from the stratified population.

5 The population was stratified for new and renewal security screenings into four scope periods due to the impact of the pandemic on the security screening process and the Department's decision to work remotely. The four scoped periods are as follows: 1) pre-pandemic; 2) initial period of the pandemic – Department's decision for remote work; 3) Treasury Board Secretariat's temporary variation to the security screening procedure (criminal record check); and 4) post-TBS temporary variation and the Department's return to 90 Elgin.

Date modified:
2023-09-26