Department of Finance Canada | Ministère des Finances Canada

AUDIT OF SAFEGUARDING OF SENSITIVE INFORMATION

Audit Report

Prepared by:
Internal Audit Directorate

December 2018

Canada

©Her Majesty the Queen in right of Canada (2019)

All rights reserved

All requests for permission to reproduce this document
or any part thereof shall be addressed to
the Department of Finance Canada.

Cette publication est également disponible en français.

Cat. No.: F2-270/2019E-PDF
ISBN: 978-0-660-29587-9

TABLE OF CONTENTS

EXECUTIVE SUMMARY

WHAT WE EXAMINED

The objective of this audit was to provide reasonable assurance that sensitive[1] information is adequately protected by the Department of Finance Canada's (the Department) employees. The focus of this assurance engagement was to assess how the Department manages the risk of sensitive information being leaked and the Department's level of readiness to handle suspected or actual leaks[2].

To assess their adequacy, we reviewed the governance processes and structures in place (committees, defined roles and responsibilities), the training and awareness programs and activities offered to employees, and staffs' level of adherence to the Values and Ethics Code for the Public Sector and the Department of Finance Code of Conduct. We also reviewed how the Department handles wrongdoing under the *Public Servants Disclosure Protection Act* and its level of readiness to respond to leakages of confidential information.

We have included in this report reference to employees' access to sensitive classified information residing on the Budget Drive *redacted* and Budget SharePoint, the two main repositories of documents related to the Budget information used by the Department. This control was assessed during the Audit of Information Management of the Federal Budget Process; however, as it is a key area that directly impacts the safeguarding of sensitive information, we have referenced it again.

WHY IT IS IMPORTANT

The Department of Finance Canada is an information-based organization that requires and generates a significant amount of classified and sensitive information. In today's workplaces, employees have greater flexibility to work outside of the office and increased access to a wide range of sensitive corporate information and records[3]. Unauthorized disclosure of such information (intentional or accidental) can seriously impact the reputation and integrity of the Department and the government as a whole. This sensitive information must be appropriately managed and protected to minimize the risk of its loss or leakage and to maintain Canadians' confidence in the public service.

WHAT WE FOUND

The Department has governance processes and structures in place to provide oversight and to safeguard its sensitive information. This is exercised through three key senior management committees,

specifically the Executive Committee, the Management Advisory Committee and the Departmental Coordinating Committee. All three committees provide oversight over the Department's programs and operations. However, the audit was unable to conclude on the effectiveness of these committees in providing this oversight due to the limited availability or absence of Records of Decisions.

The Department has established a Values and Ethics Program, a platform that supports employees in integrating values and ethics into their daily activities and reinforces a culture of accountability. The program includes a training and awareness component that is designed to maintain a strong ethical culture throughout the Department and enhance employees' knowledge and understanding of their responsibilities in protecting sensitive information. To assess the level of employee awareness of these responsibilities, the audit team, in collaboration with the Office of Values and Ethics, conducted an employee Safeguarding of Sensitive Information and Values and Ethics Climate Survey that revealed positive results.

The audit also noted that the Office of Values and Ethics undertakes a number of initiatives to help identify, assess, and communicate risk information across the organization and to guide the development of awareness and training activities within its Values and Ethics Program. Nevertheless, briefings to senior management committees on the results of these initiatives and Values and Ethics issues are generally ad hoc and at the discretion of the Director of Office of Values and Ethics.

As departmental employees have access to sensitive information, there is the potential to use non-public information for personal benefit. To mitigate this risk, the Office of Values and Ethics has developed a mandatory annual reporting process that requires all public servants working in the Department of Finance[4] to acknowledge their obligations under the Department of Finance Code of Conduct and to report their assets to determine whether there is a potential conflict of interest. The Office of Values and Ethics reviews these reports to ensure that there are no real, apparent, or potential conflicts of interest between employees' official duties and their private interests. This process excludes contractors, Governor-in-Council appointments, and employees of other government departments.

The audit found that between April 1, 2017 and March 31, 2018, about 18% of the employees sampled did not submit a report within the required two month reporting timeframe established for each branch. Active follow-up was required to ensure that all employees submitted their annual report as a term and condition of employment. Recently, the Office of Values and Ethics has taken steps to improve their annual monitoring process to ensure better reporting coverage.

With regards to the implementation of the *Public Servant Disclosure Protection Act (PSDPA*), the Department has a well-defined Wrongdoing Disclosure Process which outlines all possible avenues to explore should a disclosure of a wrongdoing be made. Due to the fact that there were no reported wrongdoings during the audit period, the audit could not conclude on the current effectiveness of the disclosure process.

The audit also found that the Department does not have a documented protocol that outlines the steps to be followed in the unlikely event that sensitive information is leaked.

The audit found that there is an established process in place to obtain access to the Budget Drive *redacted* and Budget SharePoint, the key networks that contain sensitive information created for the Federal Budget (Budget). However, a high number of information technology (IT) employees within the Department and Shared Services Canada staff, possess 'elevated' security profiles which allow them to access sensitive Budget information in the "collaboration" area within Budget SharePoint.

Kari Swarbrick
Chief Audit Executive

BACKGROUND

1. The Department of Finance Canada's (the Department) reputation and its ability to develop and implement strong policies and programs, provide advice, as well as execute critical government operations, is dependent upon its readiness to protect sensitive, classified data and to handle a security breach in the event it occurs. Potential information leakages and the Department's level of preparedness to deal with a security breach are great risks to the Department. An audit in this area was identified in the 2017–2020 Risk-Based Audit Plan that was approved by the Deputy Minister on June 9, 2017, to focus on how the Department prevents leakages of confidential information (excluding IT Security).

2. The Office of Values and Ethics consists of three staff members (a Director, a Senior Officer, and an Administrative Coordinator). They regularly liaise with all nine branches and particularly with the Corporate Services Branch, which has functional responsibility for many key areas and activities that support and promote the importance of values and ethics - e.g. human resources, information management, information technology (IT), and financial management. The Office of Values and Ethics also provides ongoing support to the Values and Ethics Advisory Network (comprised of branch representatives), which serves as a forum for ongoing dialogue on values and ethics issues, challenges and training needs.

AUDIT OBJECTIVE AND SCOPE

OBJECTIVE

3. The objective of this audit was to provide reasonable assurance that sensitive information is adequately protected by the Department of Finance Canada's (the Department) employees. The focus of this assurance engagement was to assess how the Department manages the risk of sensitive information being leaked and the Department's level of readiness to handle suspected or actual leaks.

4. Specifically, during the audit, we assessed whether:

   - The Department had an effective governance system in place to provide oversight and safeguard of sensitive information;

- The Department had adequately communicated relevant procedures (including guidance and training) to staff to mitigate the risk of unauthorized dissemination of sensitive information;
- The Department had a process in place to ensure that all employees adhere to the Values and Ethics Code for the Public Sector and the Department of Finance Code of Conduct (the Codes) with respect to the safeguarding of sensitive information;
- Employee access to sensitive and classified information systems and classified information was effectively controlled;
- The Department had an established process in place to handle wrongdoing under the *Public Servants Disclosure Protection Act*; and
- The Department had a process in place to handle suspected or actual information leaks.

SCOPE

5. The audit covered the period from January 2016 to March 2018 and included the following key areas to safeguard sensitive information:

   - Governance;
   - Training and Awareness;
   - Adherence to the Values and Ethics Code for the Public Sector and the Department of Finance Code of Conduct; and
   - Handling of wrongdoing under the *Public Servants Disclosure Protection Act.*

6. The audit did not assess the following areas:

   - Physical Security – this area was assessed in the Audit of Information Management of the Federal Budget Process and in the Audit of Physical Security conducted in 2017;
   - IT Security – this area was assessed in the Audit of Access to Information – Systems and Processes published in May 2015;
   - Business Continuity Planning – this area was assessed in the Security Audit of the Business Continuity Planning Program published in August 2016; and
   - Security measures of other government departments, agencies and third party service providers that have access to the Department's sensitive information.

APPROACH

7. The audit was conducted by the Department's Internal Audit Directorate.

8. During the conduct of this audit, we:

   - Reviewed relevant documents, including the Treasury Board policies;
   - Reviewed departmental information management and access control guidance;
   - Reviewed Records of Decisions from various senior management committees meetings;
   - Interviewed individuals from the Office of Values and Ethics, Human Resources Division, and the IT Division to gain an understanding of the processes;
   - Surveyed employees to measure the level of employee awareness of their responsibilities related to the safeguarding of sensitive information;
   - Tested a sample of employee's Affirmation/ Confidential Reports and a sample of consultant contracts; and
   - Conducted a review of employees' systems access controls.

9. Fieldwork for this audit was substantially completed on October 21, 2018.

OPINION

10. Sufficient and appropriate procedures were performed and evidence gathered to support the accuracy of the audit conclusion. The audit findings and conclusion were 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.

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

STATEMENT OF CONFORMANCE

12. 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.

DETAILED FINDINGS AND RECOMMENDATIONS

GOVERNANCE PROCESSES AND STRUCTURES

13. Governance is defined as the combination of processes and structures implemented by an organization to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives. We expected the Department to have established adequate and effective governance processes and structures that provide oversight and safeguard sensitive information. This would include establishing committee and reporting structures, and defining clear roles and responsibilities to ensure the effective management and monitoring of departmental controls designed to protect sensitive information.

14. The governance structure that provides oversight over the Values and Ethics Program within the Department consists of three senior management committees: the Executive Committee (EXEC), the Management Advisory Committee (MAC) and the Departmental Coordinating Committee (DCC).

15. The responsibilities for the interpretation and administration of the Codes reside with the Office of Values and Ethics, while the Corporate Services Branch manages the Informal Conflict Management System (ICMS) and the formal complaint processes. However, there is coordination between the Office of Values and Ethics and the ICMS, as employee issues are often brought to the Office of Values and Ethics' attention first and may be referred to ICMS, if necessary.

16. The Director of Values and Ethics (Director) reports administratively to the Assistant Deputy Minister of Law (ADM-Law), and functionally to the Deputy Minister (DM). The Director has monthly bi-lateral meetings with the ADM-Law on issues that he determines require discussion. The Director reports to the Deputy Minister, on a case-by-case basis, on issues that cannot be resolved at the lower level.

17. Values and ethics issues and program information are brought to senior management committees' attention when the Director determines that there is a need to update these committees on significant program issues or to obtain management approval on key initiatives. There is no consistent periodic reporting on the overall program's results at this level; briefings to senior management committees on values and ethics issues are generally ad hoc and at the initiative of the Director. A regular scheduled update on values and ethics issues is not part of any of the committees' forward agendas.

18. The EXEC is the final and most senior level committee for the approval of matters related to corporate management policies, stewardship, and recommendations made by the MAC and DCC. Key strategic information, such as proposals for the staffing and classification of EX positions and quarterly financial reporting, is also presented to the EXEC members. This Committee is chaired by the Deputy Minister and composed of the Associates, Assistant Deputy Ministers (ADM) from all branches, the DM's Chief of Staff and the Chief Financial Officer. The MAC's primary purpose is to discuss, reflect, and agree on corporate management objectives, priorities, and deliverables, at a strategic level. It is chaired by an Associate Deputy Minister and composed of employees from all branches, Senior Leaders, and Champions. The DCC is a discussion forum for implementation challenges and comparative practices within the Department. It is chaired by an Associate ADM selected by the EXEC and has Associate ADM (or equivalent) representation from each branch, as well as the DM's Chief of Staff. The Chair of the DCC reports to the EXEC with a frequency and in a manner decided by the EXEC.

19. The audit found that Records of Decisions are not prepared from either the EXEC or the DCC meetings. Records of Decisions are important because they formally define roles and responsibilities, provide reference information for subsequent discussions, actions, and follow-up.

20. We can conclude that the Department has governance processes and structures in place to provide oversight and safeguard sensitive information but the effectiveness of oversight could not be fully assessed due to the absence of records of decisions.

> **Recommendation #1**
> The Chairs of the Executive Committee and the Departmental Coordination Committee should document key decisions made during their meetings.

TRAINING AND AWARENESS ACTIVITIES

21. Training and awareness are key activities and tools to ensure that departmental employees' understand how to maintain the confidentiality of information. We expected the Department to have established adequate and effective training and awareness activities to communicate Values and Ethics and relevant policies within the organization.

22. The audit found that the Department made consistent efforts to communicate Values and Ethics and increase employees' awareness, through various activities and training opportunities. These include:

- **TV posters:** Messages are posted on TV screens throughout the Department to increase awareness of Values and Ethics, including duty of loyalty, social media awareness, and post-employment obligations.
- **Intranet and e-mail communications:** Messages and info bulletins are sent by the Deputy Minister and the Director of Values and Ethics to convey Values and Ethics related information to all employees. These messages are sent via e-mail and posted on the Department's 'InfoSite'. Special messages of precaution are also sent during the holiday seasons and Federal Budget period to increase awareness of Values and Ethics risks when employees are more susceptible to those risks.
- **Intranet resources:** Key documents, tools, guidance, and training are posted on the Department's 'InfoSite'.
- **Annual mandatory reporting of potential conflict of interest:** All employees are required to complete and submit to the Office of Values and Ethics a mandatory Affirmation/Confidential Report at the time of their employment and annually thereafter, to acknowledge that they have read and understood the Department of Finance Code of Conduct. For incumbents, employees are advised of their annual reporting requirement via e-mail. Reminder e-mails are sent toward the end of the reporting period and in cases of non-compliance after the deadline, the Office of Values and Ethics notifies the employee's Assistant Deputy Minister.
- **Letter of offer:** All letters of offer contain information about employees' rights and obligations with respect to participation in political activities and compliance with the Codes (both outlining the expected behaviour in all activities related to employees' duties) as a condition of employment.
- **Post-employment obligation:** All employees leaving the public service are notified of post-employment obligations in exit letters.
- **Online courses:** Within six months of their appointment, all new employees to the Public Service must complete a mandatory online orientation session offered by GC Campus that includes a Values and Ethics segment. Additional online courses related to the safeguarding on sensitive information that are strongly recommended (e.g. regarding security awareness, records management) are also available through the GC Campus. While employees' uptake of the GC

mandatory training is not systematically monitored, progress reports are requested from the Human Resources division on an "as needed" basis (e.g. to report results against the Management Accountability Framework indicators).

- **Awareness sessions:** The Office of Values and Ethics conducts various training and awareness sessions that are developed based on the questions, consultations, and feedback received from employees, as well as specific requests from managers.
- **Computer pop-ups:** Periodic computer screen pop-ups prompt employees to acknowledge having read and understood the Department of Finance Code of Conduct.

23. In order to measure the effectiveness of the awareness program, the Office of Values and Ethics conducted Values and Ethics Employee Climate Surveys in 2011, 2014, and 2018. The results from these surveys provided input into the development of the Values and Ethics Action Plan and Results Framework (Values and Ethics Action Plan), as well as messages, training, guidelines, and awareness sessions. The results were also used to target areas of improvements and increase the level of awareness. Additionally, the Office of Values and Ethics conducted information sessions and used participants' feedback to develop training material for subsequent sessions.

24. Furthermore, in coordination with the Office of Values and Ethics, we conducted an employee survey on safeguarding of sensitive information and the Values and Ethics climate. The results showed that 96.62% of the 148 survey respondents were aware of their responsibilities with regard to handling sensitive information. Additionally, 88.5% of the employees surveyed indicated that they had a good understanding of the Department's 'need-to-know' requirements. This result is in line with the results obtained in the 2014 Employee Climate Survey.

25. After reviewing all the communication and training efforts made by the Department and the results from the surveys, we determined that there is an adequate level of effort in communicating Values and Ethics to all staff within the organization.

ADHERENCE TO THE VALUES AND ETHICS CODE FOR THE PUBLIC SECTOR AND THE DEPARTMENT OF FINANCE CODE OF CONDUCT

26. The Codes outline the values and expected behaviors that guide public servants in all activities related to their professional duties. We expected that the Department had processes in place to ensure that all employees' adhered to the Codes with respect to safeguarding of sensitive information.

27. The audit noted that the Office of Values and Ethics has adopted a number of positive initiatives to ensure adherence of the Codes and to improve the risk management of the Values and Ethics Program. These included the development of a Values and Ethics Action Plan; participation in various Values and Ethics networks; involvement in the Department's integrated planning process; and a mandatory annual reporting process to monitor the conflict of interest risk.

28. **Values and Ethics Action Plan:** The Action Plan is a Deputy Minister approved three-year plan updated annually, that serves as a road map for Values and Ethics activities within the Department. The most recent Plan was presented to the Executive Committee in May, 2018. It is developed and continuously revised based on various inputs, including results of the Public Service Employee's Survey and the Values and Ethics Employee Climate Survey; employee requests for information/guidance on values and ethics issues; and feedback form completed from Values and Ethics training sessions. This information is also used to develop and revise awareness messages, guidelines, and training content. The intent of this this framework is to identify, assess, and communicate risk information in a timely manner across the organization to enable staff, management, and the senior management committees to carry out their responsibilities. However, we noted that the overall results of the Values and Ethics Program, including the outcomes of the annual review of employees' Affirmation/Confidential reports, as well as risk information related to the day to day operations, are not communicated to senior management committees on a regular basis.

29. **Participation in Values and Ethics networks and involvement in the Department's integrated planning process**. The Director of Values and Ethics and the Program Advisor participate in inter-departmental networks, webinars, and external initiatives to learn and share best practices and to ensure that the Department's Values and Ethics Program is aligned with the Public Service wide initiatives. In addition, the Office of Values and Ethics participates in the annual development and update of significant corporate documents, such as the Departmental Plan, Integrated Business Plan, Corporate Risk Profile, and Human Resource Plan, by identifying Values and Ethics risks and underlining the need for a strong Values and Ethics culture.

30. **Mandatory annual reporting process to monitor the conflict of interest risk.** The Office of Values and Ethics has developed a process that requires all employees to report their assets to determine whether there is a potential conflict of interest (e.g. arising from financial investments and the transfer of economic benefit or from messages and information transmitted via the Internet and

other media). Given the Departmental employees' access to sensitive information, the potential use of non-public information for personal gain could result in a conflict of interest situation. To mitigate this risk, the Office of Values and Ethics requires all new departmental employees to complete a mandatory annual Affirmation/Confidential Report within 60 days of the effective date of their appointment. This report includes all publicly traded securities, outside activities and employment. Afterwards, employees are required to complete and submit this form on an annual basis or any time there is a change in circumstances (e.g. changes in duties, assets, etc.). Once completed, the reports are reviewed by the Director of Values and Ethics to determine the absence of, or potential conflict of interest, based on an established set of guidelines. When a potential conflict of interest is detected, discussions are held with the employee in question and could result in one of three options: 1) divestment by sale; 2) conversion to blind trust; or 3) asset freeze. The decision is made in collaboration with the affected employee, and for the most part, employees agree to divest. If a given employee disagrees to divest and believes that there is no conflict of interest, the Director of Values and Ethics sends a memorandum to the Deputy Minister for his decision.

31. The audit selected a sample of 132 employees with an 'active' status in the PeopleSoft database between April 1, 2017 and March 31, 2018, to test for compliance with their obligation to acknowledge their obligations under the Codes and disclose any potential conflict of interest in a timely manner. The audit tests revealed that approximately 70% (92) of these employees submitted an Affirmation / Confidential Report, as required. The variance is explained as followed:

- **No Affirmation / Confidential Reports to review:** For about 18% of the remaining employees, we could not find evidence of reports being submitted to the Office of Values and Ethics. In more than a half of these cases, the reason was that the Office of Values and Ethics relied solely on PeopleSoft for employees' records at the time to identify those employees who needed to complete and submit their declaration forms; this database that was not updated often enough to allow for a timely identification of newly hired employees, secondments, casuals, or students, therefore some of them were not reminded about their annual reporting obligations.
- **Departures:** In 12 cases (about 9% of the employees in the sample), we could not assess compliance with the conflict of interest reporting requirement because the employees left the Department before the end of the conflict of interest reporting period.
- **Different disclosure processes:** Four (4) employees in the sample (3%) followed a different disclosure process: one (1) Ministerial staff member (Governor in Council appointee) required to report to the Conflict of Interest and Ethics Commissioner instead of the Department of Finance

and 3 contract consultants required to acknowledge their obligations for safeguarding of sensitive information through their contractual agreements. We reviewed a random sample of ten (10) professional service contracts under the audit period and found that all contracts but one included specific clauses or separate terms and conditions to cover confidentiality and conflict of interest requirements under the Values and Ethics Code for the Public Service.

32. Since December 1st, 2017, the mandatory annual reporting process to monitor the conflict of interest risk has been improved to ensure that the Values and Ethics database is updated regularly to capture all active employees, including students, new staff, and casual employees. The Office of Values and Ethics is now receiving Arrival and Departure Forms from IT Services on a daily basis. This allows them to cross-reference the Values and Ethics database against the PeopleSoft database and to ensure better coverage for monitoring compliance with the conflict of interest reporting requirements.

33. Overall, the Department has a good process in place to mitigate the risk of non-adherence to the Codes. Nevertheless, the overall outcomes of the Values and Ethics Program as a whole, including results of the annual review of employees' Affirmation/Confidential reports and follow up efforts, outcomes of training and awareness activities, and key information on the day to day operations, were not consistently reported to senior executive committees. As already mentioned above, the Office of Values and Ethics has been taken steps to improve the annual monitoring of conflict of interest declarations. However, we would expect that the results of this process, along with information on the program's overall performance, the sufficiency of resources and perhaps succession planning, is communicated to the Executive Committee on a regular basis.

Recommendation #2

The Director of Values and Ethics should periodically review the relevance and sufficiency of performance information collected and monitored and report annually to the Executive Committee on:

- the overall results of the Values and Ethics Program;
- the outcomes of the annual review of employees' Affirmation/Confidential reports;
- operational risks (e.g. sufficiency of resources, succession planning, etc.); and
- other program performance information, as deemed necessary.

HANDLING OF WRONGDOING UNDER THE PUBLIC SERVANTS DISCLOSURE PROTECTION ACT

34. The core responsibility of the Department is to develop the Federal Budget and the Fall Economic Statement, as well as provide analysis and advice to the Government of Canada on economic, fiscal and social policy; federal- provincial relations, including the transfer and taxation payments; the financial sector; tax policy; and international trade and finance. Hence, the Department's employees have access to an abundancy of sensitive information and the risk of wrongdoing within the organization is very high.

35. As per the *Public Servants Disclosure Protection Act (PSDPA)*, wrongdoing is defined as:

- a contravention of any Act of Parliament or any Act of the legislature of a province, or of any regulations made under any such Act, other than a contravention of section 19 of this Act these Acts;
- a misuse of public funds or a public asset;
- a gross mismanagement in the public sector;
- an act or omission that creates a substantial and specific danger to the life, health or safety of persons, or to the environment, other than a danger that is inherent in the performance of the duties or functions of a public servant;
- a serious breach of a code of conduct established under section 5 or 6; and
- knowingly directing or counselling a person to commit wrongdoing as defined above.

36. We expected that the Department had established and defined a wrongdoing disclosure process to handle wrongdoing under the *PSDPA*.

37. We noted during the audit that the Department has an established and defined wrongdoing disclosure process, which outlines all possible avenues to be followed when disclosing wrongdoing. When an employee wishes to disclose a potential wrongdoing, the employee meets with a Disclosure Protection Officer (the Director of Values and Ethics) to discuss the nature of the potential wrongdoing. An informal conversation takes place in confidence to determine whether the perceived wrongdoing actually meets the definition of wrongdoing. The audit team was informed that during the audit period there were only three (3) cases reported but none of them met the definition of a wrongdoing and were, therefore, referred to other processes, such as the Informal Conflict Management System (ICMS). The Disclosure Process is available to all employees on the Department's InfoSite.

38. Due to the fact that there have not been any valid wrongdoings reported during the audit period, the audit was unable to conduct further audit tests to conclude on the effectiveness of the wrongdoing disclosure process.

Information Leaks

39. The audit found that while there are measures in place to prevent leakages of information, the Department does not have written procedures to formally identify stakeholders' responsibilities and the actions to be taken following suspected or actual information leaks to outside sources (excluding breaches to IT systems). Departmental officials indicated that in such situations there is an informal process in place, whereby key divisions and branches within the Department (IT Security, Labour Relations, and Law Branch) and possibly other federal organizations (e.g. the Royal Canadian Mounted Police, the Privy Council Office) could be involved and an investigation would be initiated, if necessary; however, a formal protocol was not formally documented.

40. In conclusion, the Department has an established wrongdoing disclosure process in place to address employee misconduct and to handle wrongdoing. However, it would benefit the organization if formal written procedures were in place to identify the actions to be taken in the event of suspected or actual leakages of sensitive information.

> **Recommendation #3**
>
> The Departmental Security Officer should document and disseminate the process for handling an actual or suspected leakage of sensitive information to ensure timely identification and involvement of key players in the investigation, steps to follow, and actions to be taken.

EMPLOYEE NETWORK ACCESS CONTROLS

41. During the Audit of Information Management of the Federal Budget Process, we noted that a high number of IT employees within the Department and staff from Shared Services Canada (SSC) had 'elevated' security profiles, which allowed them to have access to sensitive Budget information. As this is another key area that directly impacts the safeguarding of sensitive information, we decided to reference it again in this report.

42. For the purpose of this audit, the sensitive information that is referred to in this section includes only the information residing on the Budget Drive *redacted* and Budget SharePoint (classified),

the two main repositories of documents and Budget information used by the Department. Access to classified information on all other protected or classified information in the networks shared drives are out-of-scope for this audit.

43. The audit noted that there is an established process to obtain access to these two networks. Access needs to be approved by branch Budget Coordinators and again verified by the IT Help Desk before a requestor could be granted access. However, the audit found that a high number of IT employees – thirty (30) within the Department and twenty four (24) staff from SSC - had 'elevated' security profiles, which allowed them to have access to the "collaboration area", an open space on the Budget SharePoint network that contains sensitive Budget information shared during the Budget season.

44. The more people have access to confidential information, the more opportunities there are for information leakages. It is important that the Department conducts regular reviews of the number of IT staff with elevated security profiles and work with SSC to identify ways to limit the layers of access control for these employees.

45. Employees' access to the network is recorded; however, reconciling access on the network drives is neither straightforward nor easy. Within the Department, reconciling access on SharePoint is much easier than on the Budget Drive *redacted*, because SharePoint has a detailed audit trail that is easy to access. For the Budget Drive *redacted*, interpretation of the audit trail is more challenging; access logs are kept, but reading logs is a time consuming exercise and can be difficult to decipher. As the Department is gradually migrating to SharePoint, more efficient security audit trail tools might be needed to improve the interpretation of network access. This would increase the Department's efficiency in addressing information leaks in the event they occur.

Recommendation #4

The Chief Information Officer should conduct periodic reviews of the number of IT staff with elevated security profiles and reduce this number where appropriate.

CONCLUSION

46. Overall, the Department has effective governance processes and structures, training and awareness strategies, and access control processes in place to support the protection of sensitive information

by departmental employees. The Department has established a Values and Ethics Program that supports and guides employees in complying with the highest ethics and standards of conduct in their daily activities. In addition, the Department has processes in place to handle wrongdoing under the *Public Servants Disclosure Protection Act*. The issues raised in this audit report are meant to provide management with insight in what could be improved in these areas, as part of a continuous improvement exercise.

47. Organizational commitment to Values and Ethics and the principles of responsible stewardship play a key part in the protection of sensitive information. While there are a number of internal controls in place to support the protection of sensitive information by departmental employees, certain elements of the control framework could be improved. These include:

- better documentation of decisions made by the senior management committees regarding values and ethics issues;
- annual reporting to the Executive Committee on the overall outcomes of the Values and Ethics Program;
- documentation of the process to be followed in cases of actual or suspected leakages of sensitive information; and
- finding the optimal balance between security requirements and the level of access granted to IT employees.

RECOMMENDATIONS, MANAGEMENT RESPONSE AND ACTION PLAN

Overall Management Response	
Management agrees with the findings and the recommendations.	
Recommendations	***Management Response and Action Plan***
1. The Chairs of the Executive Committee and the Departmental Coordination Committee should document key decisions made during their meetings.	**Management Response:** The Chairs of the Executive Committee (EXEC) and the Departmental Coordination Committee (DCC) agree with the recommendation. **Action Plan:** A common and consistent approach will be developed for recording decisions for action items (i.e., items presented to the committees for approval). Records of decisions will be maintained by the Deputy Minister's Chief of Staff for EXEC and by the committee secretary for DCC, and will be disseminated to Committee members. **Lead:** Chairs of EXEC and DCC **Target Date:** December 2018
2. The Director of Values and Ethics should periodically review the relevance and sufficiency of performance information collected and monitored and report annually to the Executive Committee on: · the overall results of the Values and Ethics Program; · the outcomes of the annual	**Management Response:** The Director of Values and Ethics agrees with the recommendation. **Action Plan:** Reports on the overall results of the Values and Ethics Program, including values and ethics issues - e.g. the number of conflicts of interest, challenges, - will be presented to the Executive Committee on an annual basis. The most recently approved Values and Ethics Action Plan

review of employees' Affirmation/Confidential reports; · operational risks (e.g. sufficiency of resources, succession planning, etc.); and · other program performance information, as deemed necessary.	will be updated to reflect the need for an Annual report to the Executive Committee. **Lead:** Director of Values and Ethics **Target Date:** A report is currently being prepared for presentation to the Executive Committee before the end of 2018. Annual reports will be presented in May-June of each fiscal year thereafter. The Values and Ethics Action Plan is currently being updated.
3. The Departmental Security Officer should document and disseminate its process for handling an actual or suspected leakage of sensitive information to ensure timely identification and involvement of key players in the investigation, steps to follow, and actions to be taken.	**Management Response:** The Departmental Security Officer agrees with the recommendation and will develop a written protocol for handling an actual or suspected leakage of sensitive information for the reference of Security Services. **Action Plan:** A written protocol will be developed. **Lead:** Deputy Departmental Security Officer **Target Date:** December 2018
4. The Chief Information Officer should conduct periodic reviews of the number of IT staff with elevated security profiles and reduce this number where appropriate.	**Management Response:** The Chief Information Officer agrees with the recommendation as it is a best practice to review on a periodic basis the number of elevated accounts granted to IT personnel. It is important to note however that the Department of Finance is a small organization with a limited number of IT specialists, and the traditional segregation of duties for the management of information systems could put

	IT and departmental operations at risk. Further, the organizational structure of Shared Services Canada (SSC), with multiple service lines (e.g., Storage Operations, Network Security, Operating Systems Operations), contributes to the number of elevated accounts. **Action Plan:** - On a monthly basis, the IM/IT Client Service Desk will produce a report detailing the list of elevated accounts granted to SSC employees, including the employee name, the employee manager's name, the service line supported and the FIN IT assets provided to the employee to perform the work; - On a quarterly basis, the IM/IT Client Service Desk will request the Department of Finance IT managers and the SSC Service Delivery Manager to confirm the business requirements for elevated accounts and update the information, as required. This information will be communicated to the departmental IT Security Coordinator. **Lead:** Chief Information Officer **Target Date:** March 31, 2019

ANNEX A: AUDIT CRITERIA

The following audit criteria were used in the conduct of this audit:

- Governance is exercised to provide appropriate oversight over the safeguarding of sensitive information;
- Training and awareness programs are effectively deployed to enhance employees' knowledge and understanding of their responsibilities in protecting sensitive information;
- Sound values and ethics practices are implemented to safeguard sensitive information; and
- Established processes are in place to address employee misconduct and information leaks.

ANNEX B: ACRONYMS

Acronym	Name in Full
ADM	Assistant Deputy Minister
DCC	Departmental Coordinating Committee
DM	Deputy Minister
EXEC	Executive Committee
ICMS	Informal Conflict Management System
IT	Information Technology
MAC	Management Advisory Committee
PSDPA	Public Servant Disclosure Protection Act

[1] Sensitive information is considered classified information.
[2] The overall objective encompasses intentional and accidental leakages and excludes IT security external breaches.
[3] Examples include: economic, fiscal, proprietary, commercial, protected through Confidentiality Agreements, legal, personal, etc.
[4] The Department of Finance Code of Conduct refers to all public servants working in the Department of Finance, including indeterminate and term employees (full and part-time), persons on secondment to the Department, casuals, students and staff on leave with or without pay.