Office of the Superintendent of Financial Institutions Canada
Bureau du surintendant des institutions financières Canada

Office of the Superintendent of Financial Institutions

Internal Audit Report on
Office of the Chief Actuary -
Information Management and Privacy

June 2015

OSFI
BSIF

Canada

Table of Contents

1. Background

Introduction

The Office of the Chief Actuary (OCA) was created to provide actuarial and other services to the Government of Canada and provincial governments who are Canada Pension Plan stakeholders. OCA was established within the Office of the Superintendent of Financial Institutions Canada (OSFI) as a separate unit and while the Chief Actuary reports to the Superintendent of OSFI, the Chief Actuary is solely responsible for the content and actuarial opinions in reports prepared by OCA. This structure promotes independence, which helps ensure impartial professional judgment in discharging OCA's mandate.

OSFI Internal Audit periodically conducts assurance work to determine whether OCA's risk management, control processes, and governance, as designed and represented by management, are adequate and functioning in a manner to ensure risks are appropriately identified and managed, and in compliance with applicable policies and procedures.

The audit of OCA was recommended by the OSFI Audit Committee and approved by the Superintendent for inclusion in OSFI's 2014-15 Internal Audit Plan. This report presents the results of the audit based on audit work completed in March 2015.

This report was presented to the OSFI Audit Committee on June 19, 2015 and was subsequently approved by the Superintendent. OCA management has reviewed this report and provided their responses along with action plans.

Why this audit is important

OCA contributes to a financially sound and sustainable Canadian public retirement income system through the provision of expert actuarial valuation and advice to the Government of Canada and to provincial governments that are Canada Pension Plan stakeholders. OCA conducts statutory actuarial valuations of various pension plans. In the event of a bill being introduced before Parliament that has a significant impact on the financial status of a public pension plan or social program falling under the statutory responsibilities of the Chief Actuary, OCA must submit an actuarial report valuing this impact to the appropriate minister. OCA also provides the relevant government departments with actuarial advice on the design, funding, and administration of their plans.

OCA receives data from various sources including data from other government departments and agencies. Some files contain age, marital status, salary, and medical information, etc. OCA is responsible for collecting, analyzing, storing, protecting and properly disposing of this data.

2. About the Audit

Audit Objective

The objective of the audit was to assess the adequacy of information management and privacy practices.

Audit Scope

The audit covered the operational activities related to the mandate of and under the direct control of OCA, as they pertain to the management and protection of protected and classified information. Areas covered included training and awareness, applicable policies, directives and procedures, internal control design and effectiveness, and monitoring and oversight.

Audit Approach

The audit evaluation criteria used for assessing OCA are based on the internationally recognized Enterprise Risk Management – Integrated Framework recommended by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

The approach to conducting the audit included interviews and process walkthroughs with the OCA team, testing of controls over information management practices, and examination of documents such as training material and applicable OSFI policies and procedures.

Statement of Conformance

The audit was conducted in conformance with the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing, consistent with the Treasury Board Secretariat (TBS) Policy on Internal Audit and the Internal Auditing Standards of the Government of Canada, as supported by the results of the Quality Assurance and Improvement Program.

3. Conclusion

Audit Conclusion

Controls and monitoring practices over information management need to be enhanced. OCA operates under OSFI's information management and privacy policies and procedures but some employees do not always adhere to them and in some instances may not even be aware of them. Most employees were unable to refer to specific information management policies and procedures and stated that they would benefit from additional information management training.

In the rare instances where classified information is received by OCA, the information is retained on the network, which is only approved to host information up to Protected B level. A few employees who use the information do not have the necessary security clearance levels, and some employees have access to information of programs they do not have responsibility for. OCA's practices around data access, transmission, storage, and disposal need to be strengthened to mitigate the risk of information leakage.

OCA is a small and independent area within OSFI. OCA does not pay for OSFI's support in most areas of information management though roles and responsibilities of each party is not very clear other than in the area of computer lifecycle management. Information management and privacy is complex. OCA needs to adhere to numerous TBS policies and directives with very limited support and knowledge. OCA demonstrates a culture of wanting to do the right thing, and commits to addressing issues once it becomes aware of them.

We wish to recognize the excellent support and exchange of views with all involved in the audit. Their cooperation and contributions were invaluable to the success of the review.

4. Management Response

Management Response / Comments

This report has been reviewed by the Chief Actuary and the Managing Director of the OCA, who acknowledge its observations and recommendations.

The Management team recognizes that the observations and recommendations raised need immediate attention. The useful recommendations contained in this internal audit report will help the OCA to increase awareness of information management and privacy policies and procedures, and to mitigate the risk of information leakage by strengthening data access, storage, and transmission and retention practices.

Overall, we appreciate the thrust of the report, and agree with its observations and recommendations. The OCA will act on these as described below.

The OCA would like to thank the internal audit team who did an exhaustive review of practices regarding information management and privacy policies. It is of utmost importance that the OCA takes all necessary steps to protect the privacy of Canadians. Canadians should be confident that their administrative information is never at risk of any sort of security breach.

5. Observations and Recommendations

Observation 1 **Sensitive information**

OSFI policies, directives, and guides are intended to be consistent with TBS requirements. As a government organization, OCA needs to comply with TBS requirements. OCA does not have its own policies, directives, and guides, and relies on OSFI's. In certain cases, sensitive information received by OCA is not stored and handled in accordance to OSFI information security requirements.

Access to information must be limited to persons who have the appropriate security clearance and who have a need to know. Reliability security clearance can access protected information, and confidential, secret or top secret security clearance is required for classified information. A few OCA employees have not been screened to the necessary levels commensurate with the information they need to perform their duties. Some employees have access to network directories not required to perform their duties.

Recommendation:

OCA works with Information Management/Information Technology (IM/IT) and Security and Administrative Services (SAS) to better understand TBS and OSFI policies and procedures, in particular the OSFI Guide to Information Security and the OSFI Information Sharing Policy.

OCA also addresses the receiving, storage, and access to classified information, and ensures only employees with the necessary security clearance levels can access classified information.

Management Action Plan:

In response to these recommendations, the OCA will consult with Information Management/Information Technology (IM/IT) and Security and Administrative Services (SAS) to better understand the relevant OSFI policies and procedures. OCA will address employee's awareness through the development of clear instructions on the management of Information Security and Information Sharing, and develop the necessary tools that will help OCA Management meet OSFI information security storage and transmission requirements and control employee access to classified information.

Managing Director, Completion: March, 2016.

Continued on next page

5. Observations and Recommendations, Continued

Observation 2 **Information category and staff training**

Results of the four security sweeps conducted during the period of May 14, 2014 to February 16, 2015 show a total of 71 non-compliance incidents (42% non-compliance rate). However, it should be noted that the number of non-compliance incidents have steadily decreased over that period.

Employees’ views of what is considered classified/protected information differ. Most were unable to refer to any information management and privacy policies and procedures and would like additional information management training. Not having adequate training and security awareness may result in employees not recognizing and not properly protecting information. This could lead to information leakage.

Though supplemented by periodic reminders on the OSFI intranet, information management training is generally only part of staff orientation. The training is at a high level and focuses on financial institution data, not necessarily OCA data. Thus, OCA employees are uncertain about the category of various OCA data and the appropriate information management and privacy practices.

Recommendation:

OCA management agrees on the information category of various data OCA receives. The Privacy Act should be considered for personal information. Once the data category has been agreed to, tailored training and periodic refresher courses can be established for OCA staff. OCA can also request sweep results and target its training accordingly.

Management Action Plan:

In response to these recommendations, the OCA will, during Town Hall and staff meetings, better inform and periodically remind all OCA employees to follow the clear instructions (developed under Observation 1) regarding the relevant OSFI policies and procedures on Information Management, Information Sharing and Privacy policies. OCA will also obtain SAS sweep results to help in the development of such instructions.

Managing Director, Completion: March, 2016.

Continued on next page

5. Observations and Recommendations, Continued

Observation 3 **Data retention**

OCA does not have a record retention policy. Currently, OCA retains as much data as the storage space can handle. There are old paper files. Also, old files with sensitive information are being kept on the network. Information kept for an unnecessarily long time takes up storage space and increases the risk of information leakage. This is especially a concern for sensitive information.

Recommendation:

OCA establishes a retention policy, which includes the archiving of electronic and paper records. OCA monitors and ensures compliance to the policy. The retention period should meet legal requirements (if any), TBS and OSFI policies, Library and Archives of Canada Act, and OCA's operational needs.

Management Action Plan:

In response to these recommendations, the OCA will review existing policies and develop a retention policy which will meet legal requirements, TBS and OSFI policies, *Library and Archives of Canada Act*, and OCA's operational needs.

Chief Actuary, Completion: March, 2016.

Continued on next page

5. Observations and Recommendations, Continued

Observation 4 **Access administration and access profile**

Controls need to be established for access authorization (grant, change, and remove access) and access profile appropriateness and monitoring. For example, we noted a staff successfully made a verbal request to grant another staff access in 2014 though some Directors expect the access should only be granted with Director's written authorization. Moreover, a few OSFI employees who no longer need access to OCA files continued to have access but the access had since been removed.

Generally, employees have read and sometimes read and write access to other programs though in some cases, they do not need access to data in the other programs. Some programs have files with classified information.

Recommendation:

- OCA determines the appropriate access privileges for employees taking into consideration the pros and cons of the trusted user versus the need to know basis approach.
- OCA works with IM/IT to establish a process for access granting authorization. To ensure appropriate access privileges, OCA needs to inform IM/IT of transferred employees. Monitoring access profiles periodically can also identify any inappropriate access.

Management Action Plan:

In response to these recommendations the OCA will review each employee's access privileges and in consultation with Information Management/Information Technology (IM/IT) develop a tool or a process that will help OCA Management regularly monitor and control employee access profiles.

Managing Director, Completion: March, 2016.

Continued on next page

5. Observations and Recommendations, Continued

Observation 5 **Privacy Impact Assessment**

Privacy Impact Assessments (PIAs) are used to identify potential privacy risks of government programs/activities and help reduce those risks to an acceptable level. PIAs look at how personal information is protected as it is collected, used, disclosed, stored, and ultimately destroyed.

Except for one program, there are no PIAs nor have any assessments been performed to determine whether PIAs are required for the programs under the purview of OCA.

For the one program, which a PIA was prepared by the client, the PIA required the files to be stored on a secure server that is designated solely for these files. Currently, the files are on the same server as the rest of the OCA programs though only a few employees have access to these files. This practice might not comply with the PIA's requirement. Moreover, OCA needs to follow OSFI's retention policy until the retention requirement is finalized.

Recommendation:

OCA works with its clients, IM/IT, and Legal Services Division to determine whether PIAs are required for the other programs, and ensures compliance with the PIA requirements in effect for the one program.

Management Action Plan:

In response to these recommendations, the OCA will comply with the PIA requirements in effect for the one program and will consult its clients to determine whether PIAs are required for other programs. In the past PIAs were not developed as they are today but nevertheless the OCA data requirements were thoroughly examined by the client legal departments.

Managing Director, Completion: March, 2016.

Continued on next page

5. Observations and Recommendations, Continued

Observation 6 Information Management and Privacy Policies/Procedures/Guidelines

OCA does not have specific information management and privacy policies/ procedures/guidelines and relies on those issued by OSFI. However, in some instances, OCA employees were unaware of and not adhering to some OSFI policies and procedures such as the handling of classified information.

OCA as a government organization needs to be aware of and adhere to the applicable acts, directives, and guidelines pertaining to information management and privacy practices. OCA needs to identify the applicable OSFI policies and procedures, and develop additional guidelines to address OCA's specific needs. For example, OCA's access authorization and archive process will be different from the rest of OSFI as OCA does not use OSFI's electronic document management system (EDMS). OCA needs to ensure any policies and procedures adopted are both appropriate for its particular needs and compliant with all relevant requirements.

Recommendation:

OCA identifies all applicable information management and privacy policies and procedures and where necessary develops additional guidelines to meet OCA's needs.

Management Action Plan:

In response to these recommendations, the OCA will review all applicable information management and privacy policies and procedures and where necessary develops additional instructions (as per under Observation 1) to meet OCA's needs.

Managing Director, Completion: March, 2016.

Continued on next page

5. Observations and Recommendations, Continued

Observation 7 **Roles and responsibilities of OSFI re: OCA's information management and privacy**

There is no memorandum of understanding (MOU) between OSFI and OCA except for computer lifecycle management. There is some confusion about the roles and responsibilities of OSFI and OCA, which could result in unnecessary risk exposure due to OCA's assumption that the risks are being addressed by OSFI when they are not. OCA is not fully aware of the scope of support, service level/performance measures of OSFI's services. OCA relies on OSFI for information management policies and procedures but there appears to be some uncertainty with regards to the extent of OSFI's involvement in OCA's information management area.

Recommendation:

The Superintendent clarifies OSFI's roles and responsibilities regarding OCA's information management and privacy, and considers establishing a service level agreement that encompasses information management and privacy.

Management Action Plan:

A review is underway to determine the type and amount of IT information security that must be provided to OCA as a consequence of them being "a part of OSFI".

Based on the result of the review, an assessment of the requirements will be conducted. Low cost/low effort changes requiring IM/IT support to be implemented promptly. Final allocations to be determined in consideration of the approved IT security action plan. A biannual service agreement will be negotiated with OCA to support any incremental work.

Managing Director, Finance and Corporate Planning and Director, Information Technology Security, Completion: December, 2015.