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

Office of the Superintendent of Financial Institutions

Internal Audit on Corporate Services: Security and Administrative Services

April 2014

OSFI
BSIF

Canada

Table of Contents

1. Background

Introduction

Internal Audit conducts assurance work to determine whether the Office of the Superintendent of Financial Institutions Canada's (*OSFI's*) risk management, control, and governance processes, as designed and represented by management, are adequate and functioning in a manner to ensure risks are appropriately identified and managed, and to ensure compliance with such requirements as policies, plans, procedures and applicable laws and regulations.

The audit of Corporate Services - Security and Administrative Services (*SAS*) was approved by the OSFI Audit Committee and the Superintendent for inclusion in the OSFI 2013 to 2014 Internal Audit Plan.

This report presents the results of that audit based on audit work completed at the end of July 2013. The audit recommendations will support OSFI in sustaining a secure environment.

This report and management actions were discussed at the November 21, 2013 Audit Committee meeting with the understanding that management would present more detailed action plans and results of an independent assessment on OSFI's information technology security first line of defense at the April 2014 Audit Committee. This report was presented to the OSFI Audit Committee on April 10, 2014 and approved by the Superintendent on April 17, 2014. The Assistant Superintendent, Corporate Services and the Human Resources and Administration Division management, who have provided their management comments within this report, have also reviewed it.

Treasury Board Policies and Directives

The Treasury Board Secretariat's *(TBS')* Policy on Government Security, its Directive on Departmental Security Management and related standards govern security planning, security risk management and the roles and responsibilities for Departments and their Departmental Security Officers (*DSOs*).

The TBS Directive on Departmental Security Management states that the DSO "is to manage the departmental security program and is responsible for security planning, governance, management of security risks, monitoring and oversight, - performance measurement and evaluation, and government-wide support (Treasury Board, 2009).[1]"

Management of the departmental security program "requires the continuous assessment of risks and the implementation, monitoring and maintenance of appropriate internal management controls involving prevention (mitigation), detection, response, and recovery (Treasury Board, 2009)[2]" activities.

Continued on next page

[1] 6.1.1-6.1.15
[2] 3.3

1. Background, Continued

Governance, Risk and Control framework

Management of the departmental security program is best accomplished using an effective governance, risk, and controls framework. One way to support the framework involves the strategic implementation of three lines of defense. In this model, operational controls are the first line of defense; oversight of the operational activities and controls is the second; and independent assurance is the third.

As an example, a "*first line of defense*" that has been operationalized at the front end would be the implementation of security controls to restrict access to confidential data. SAS' responsibilities as the "*second line of defense*" would be to provide the related security framework and policies, set expectations for these controls, and thereafter oversee risk decision-making.

The DSO, housed within the SAS function, is well placed structurally to act as the second line of defense, providing security oversight by aligning strategies, risks and policies; designing policies; setting direction; ensuring compliance; and informing senior management and governance committees.

SAS's management of security intersects with other divisions, most notably the Information Management and Information Technology (IMIT) division, and other divisional management functions in providing and supporting OSFI's security programs and activities.

Continued on next page

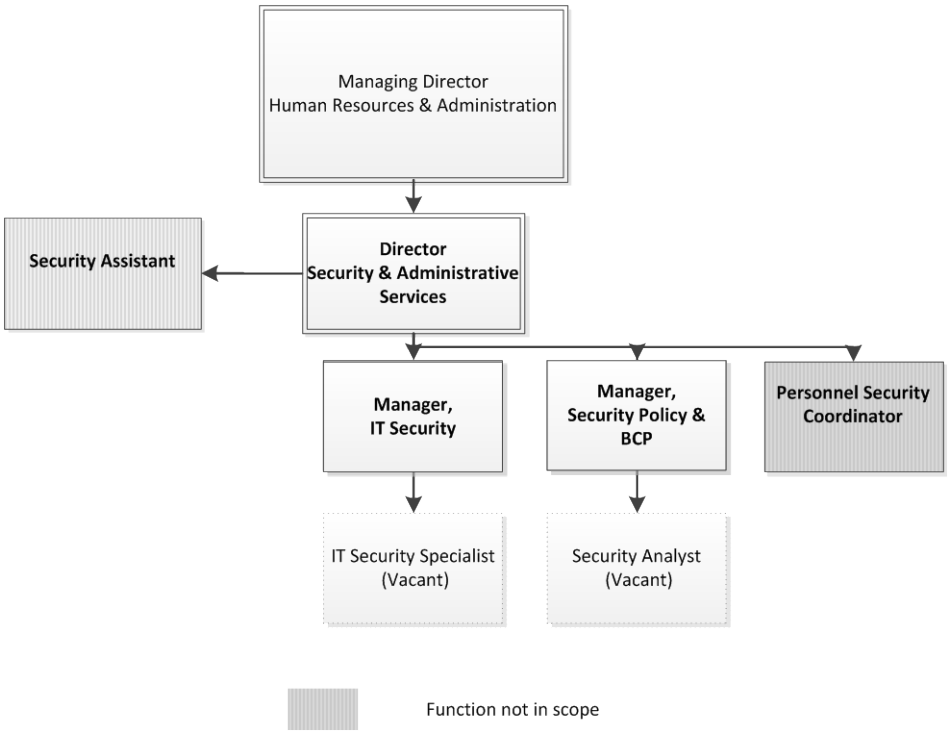
1. Background, Continued

Organizational Structure

The Director, Security and Administrative Services (*SAS*), is responsible for the SAS group. He is also the Departmental Security Officer (*DSO*) and he reports to the Managing Director Human Resources and Administration.

SAS is responsible for the delivery of 68 services as set out in its Service Catalogue of which 44 are related to security in the areas of; IT Security (13), Emergency Management (11), Contract, personnel and physical security (12), Security training & awareness (5), policies, standards and guidelines (3).

There are 6 approved full time staff that support the DSO in delivering security services, of which 4 are involved to some extent in oversight activities. Of those 4 positions, 2 were vacant at the time of the audit. The remaining 2 positions are focused on operational activities not in the audit scope.



Why this audit is important

The Security and Administrative Services *(SAS)* function was selected for an audit because of its importance in establishing a sustainable secure environment consistent with the OSFI Act (Section 22. (1)) to keep confidential any information received regarding the business or affairs of Federally Regulated Financial Institutions (*FRFIs*), and any information prepared from it.

2. Audit Objective, Scope and Approach

Audit Objective

The objective of the audit was to provide reasonable assurance that the control framework is sufficient and sustainable for Security and Administration Services to effectively meet its mandate to manage the departmental security program.

Audit Scope

The audit covered the period from April 1st 2012 to March 31st 2013 and considered planned or in progress improvements identified by management.

Based on our risk assessment and prior audit work conducted, the audit focus included SAS' business objectives over:

- security measures to categorize and manage the storage of information;
- security training and awareness;
- security incident management;
- administrative investigations;
- information technology (IT) security as it relates to integrating the standards into the systems' life cycle (infrastructure and business applications); and,
- business continuity planning (corporate and divisional).

OSFI's Departmental Security Officer (*DSO*) role, as envisioned by TBS, oversees the first line of defense i.e. the office-wide security activities. Our audit focused on the second line of defense, i.e. the DSO, and was not intended to provide assurance on the effectiveness of the security activities that may be operationalized as part of the first line of defense.

The internal audit on Information Management / Information Technology (IM/IT) Governance (2012) included a review of the structure and accountability in the management of OSFI's IT security operations and considered its intersection with SAS. The threat risk assessment recommendation from that audit was excluded from the scope of this SAS audit because management actions are in progress.

The internal audit on Information Technology Security Access (2010) addressed access to OSFI's infrastructure, systems, and business applications. Based on the satisfactory audit follow-up results, the following areas were excluded from this SAS audit: individual security screening, physical security, access control cards, and system access controls.

Continued on next page

2. Audit Objective, Scope and Approach, Continued

Audit Approach

The audit was conducted in accordance with the Institute of Internal Auditors International Standards for the Professional Practice of Internal Auditing, consistent with the Treasury Board Policy on Internal Audit.

The audit evaluation criteria (described in *Appendix I – Audit Evaluation Criteria)* sets out the elements and related components that form the basis for assessing the Security and Administrative Services control framework. These criteria are based on internationally recognized Enterprise Risk Management – Integrated Framework recommended by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). The criteria incorporate OSFI policies, directives and guidance as well as the Treasury Board Policy on Government Security and related directives and guidance.

The approach to conducting the audit included:

a) Examining the SAS control framework and underlying policy, process, service catalogue, and related procedures used for managing the security function;
b) Assessing SAS' security-related oversight practices and communications including conducting interviews with those directly involved;
c) Reviewing selected security services / programs and representative activities as set out in the Audit Scope section for the completeness, accuracy, and authorization (accountability & decision point) controls incorporated into the process;
d) Interviewing key stakeholders; and
e) Reviewing other assessments / evaluations / studies completed for strengthening and enhancing security services.

3. Conclusion

Conclusion

Security and Administrative Services (*SAS*), in housing the Departmental Security Officer role, is well placed structurally to act as a second line of defense, providing security oversight by aligning strategies, risks and policies; designing policies; setting direction; ensuring compliance; and informing senior management and governance committees.

Our audit focused on the second line of defense, i.e. the DSO, and was not intended to provide assurance on the effectiveness of the security activities that may be operationalized as part of the first line of defense.

While it is evident that much work has been done over the last several years by SAS in designing a framework to manage the departmental security program at OSFI, management will need to pull together the various components and embed the framework into OSFI operations in order to support the sustainability of the program. One of the program components that facilitates management's risk decisions and alignment with strategies and policies is the Departmental Security Plan (*DSP*) and it will need to be completed.

In my professional judgment as Chief Audit Executive, sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the conclusion provided and contained in this report. The opinion is based on a comparison of the conditions, as they existed at the time, against pre-established audit criteria that were agreed on with management. The opinion is applicable only to the entity examined. The audit was conducted in conformance with the internal audit standards of the Government of Canada, as supported by the results of the Quality Assurance and Improvement Program.

_____ _____

Chief Audit Executive, IA Date

4. Management Response

Overview

This report has been reviewed by the Director, Security and Administration Services (SAS); the Managing Director, Human Resources and Administration (HR&A) and the Assistant Superintendent, Corporate Services Sector, who acknowledge its observations and recommendations.

Responses / Comments

Management recognizes that the observations raised need immediate attention in order that OSFI can be assured of having a safe and secure infrastructure and has already set in place mitigating actions as described below.

5. Observations and Recommendations

Observation 1

Security Framework

Security and Administrative Services (*SAS*), in housing the Departmental Security Officer role, is well placed structurally to act as a second line of defense, providing security oversight by aligning strategies, risks and policies; designing policies; setting direction; ensuring compliance; and informing senior management and governance committees.

Over the past several years SAS has identified, assessed, studied and documented the design of an OSFI Security Framework. An effective Security Framework supports the oversight role. It entails a structured approach to security management allowing OSFI to effectively manage the security strategy, goals, and operational activities, which are key components of a departmental security program.

Work was still on-going during the SAS audit fieldwork on the detailed design of the Security Framework. While the design of this Security Framework was evidenced by the many evaluations and reports that have been produced over the years, it remains that this design was only partially and not formally implemented, nor were there any formal plans to effectively implement it.

Resources have been expended on a number of studies without sustained improvements to the security posture of SAS. There were four key studies since 2009, and some second line of defense actions arising from these studies remain to be effectively implemented.

SAS is having difficulties demonstrating that it is proactive and exercising a leadership role over emerging security issues. There was insufficient evidence to demonstrate how SAS, as a second line of defense, conducts continuous monitoring and assessment as to how implemented security controls are performing.

For security management to be effective, it would be expected that the steps taken to continuously monitor and assess the performance of the implemented security controls, review the security category of supported business activities, and re-assess risks and threats and the technical environments, would be documented and reported on. These activities would inform stakeholders on the departmental security program performance and its sustainability.

Continued on next page

5. Observations and Recommendations, Continued

Observation 1

Security Program Framework (Continued)

Recommendation:

SAS should demonstrate that OSFI maintains a secure environment. In order to do so, SAS needs to complete, obtain executive approval for and implement a comprehensive OSFI Security Framework.

SAS needs to ensure that the Framework is communicated to the appropriate staff and is well understood. In order to do so, it must build an overarching document that ties all of the disparate components together to provide an overview to senior management and management across the organization, with the linkages to the more detailed work instruments that security practitioners use.

Action Plan:

Historically SAS's focus has been on facilitating an effective first line of defence, i.e. helping managers and employees comply with organizational guidance on security matters. SAS recognizes the requirement for it to more effectively deliver its accountability as OSFI's second line of defence in security matters. When OSFI was smaller, a less formal approach to security risk management was followed, but management recognizes that, given significant growth in recent years and the rapid increase in cyber-security issues, more structure and oversight is required.

As a result senior management has reviewed the level of security resources and their reporting structure resulting in the creation of a new Director IT Security position within the Chief Information Officer's division. This role will provide a more focused second line of defense on IT given the increasing importance of this activity. In addition, senior management has undertaken a third party assessment of the first line of IT defense in order to gain assurance that this is operating as expected. The report concluded that OSFI has the most important technical, administrative and management security controls already in place.

An overarching Security Framework will be developed to provide the opportunity for engaging both line and senior management across the organization in identifying, assessing and addressing security in all business requirements and ensuring that both the first and second levels of accountability are clear and fully exercised.

Expected Completion Date: June 2014
Responsibility: Managing Director, Human Resources & Administration

Continued on next page

5. Observations and Recommendations, Continued

Observation 2

Security Governance

As per the Treasury Board Directive on Departmental Security Management, the Departmental Security Officer (DSO) must establish Security Governance mechanisms (e.g., committees, working groups) to ensure the coordination and integration of security activities with operations, plans, priorities, and functions to facilitate decision making.

The starting point for governance is policies that set out management expectations, risk tolerances, and risk mitigation strategies.

The 2009 Gap Analysis identified that OSFI's security policies and directives needed to be updated to align with Government of Canada policies, and include more underlying policy statements. Furthermore, there was no Business Continuity Policy drafted. In 2010, the necessary policies were updated / created in draft form and have yet to be brought to the executive for approval and subsequent implementation.

Currently, management is strengthening the DSO interaction with Information Management and Information Technology (IM/IT) in response to the IM/IT Internal Audit report. However, the mechanisms for the DSO to coordinate with the business owners regarding security are ad hoc and not formalized.

OSFI-wide Security Governance mechanisms would serve to satisfy the security management needs of OSFI to engage all security stakeholders in dialogue, in continuous improvements and ensure alignment of all security objectives, not just those in IM/IT

Recommendation:

To ensure that OSFI maintains a secure environment, SAS should:

- Obtain Executive's review and approval of the updated security-related Policies and Directives;
- Ensure that these Policies and Directives are implemented consistently across the organization;
- Implement a process for monitoring the effectiveness of these measures, including a process for regularly reporting any key current and emerging security-related issues to management; and
- Implement security governance mechanisms (e.g., committee, working group) to ensure the coordination and integration of security activities with all of OSFI and strengthen communication channels between SAS and the business owners.

Continued on next page

5. Observations and Recommendations, Continued

Observation 2

Security Governance (continued)

Action Plan:

OSFI has not been without departmental direction on security, having a variety of policy instruments in place, supported by both the TBS policy suite and ongoing involvement of the DSO in providing advice and guidance on security matters. Management agrees, though, that updated policy instruments, in concert with new OSFI policy suite guidance and revised TBS security standards will add clarity.

The revised Corporate Security Policy was approved at the October 2013 Executive Committee (EC) meeting. Following this approval, and in accordance with the recently approved OSFI Policy Framework, SAS obtained approval from the Assistant Superintendent, Corporate Services in February 2014 for the Directive on Information Technology Security and, in March 2014, the Directive on Business Continuity Management.

In addition, SAS began quarterly updates of the EC on key current and emerging security-related issues at its March 2014 meeting.

SAS will develop and recommend implementation of processes for monitoring the effectiveness of its policy instruments and work with the new IT Security division to develop appropriate governance structures by September 2014.

Expected Completion Date: September 2014
Responsibility: Managing Director, Human Resources & Administration

Observation 3

Departmental Security Plan (DSP)

OSFI has not yet completed the Departmental Security Plan (DSP). As required by the TBS Policy on Government Security[3], the Superintendent must approve a Departmental Security Plan that details decisions for managing security risks and outlines strategies, goals, objectives, priorities, and timelines for improving departmental security and supporting its implementation. This requirement took effect June 30, 2012.

The Departmental Security Officer is responsible for developing, implementing, monitoring and maintaining a DSP[4].

Continued on next page

[3] Treasury Board of Canada Secretariat. *Policy on Government Security*. 6.1.4, April 2012

[4] Directive on Departmental Security Management 6.1.1.1

5. Observations and Recommendations, Continued

Observation 3

Departmental Security Plan (DSP) (continued)

The DSP is an important security program instrument that:

- Provides an integrated view of
  - Departmental security requirements, and
  - Security threats, risks and vulnerabilities to determine an appropriate set of control objectives
- Identifies and establishes minimum and additional controls when necessary to meet control objectives and achieve an acceptable level of residual risk, and
- Outlines security strategies, objectives, priorities, and timelines for improving the department's security posture.

The DSP is a key communication tool and can provide the basis for developing work plans that support the implementation of office-wide security objectives. It supports senior management in achieving management excellence by providing a means to identify and manage operational security risks proactively. A well-prepared DSP would demonstrate what are the security needs to support the business needs, and how to achieve those needs.

Finally, the DSP can provide a basis for performance measurement, decision-making and priority setting, regularly informing senior management of the status of OSFI's Security Program effectiveness, so that appropriate management actions can be taken.

Recommendation:

A Departmental Security Plan should be finalized and presented for approval to the Superintendent.

Action Plan:

Agreed. A comprehensive DSP which can provide management with an integrated view of security requirements was finalized and presented to the EC for review, and the subsequent approval of the Superintendent, in March 2014. The DSP was guided by TBS policy instruments and is in line with the security control objectives in the TBS Directive on Departmental Security Management.

Expected Completion Date: March 2014.
Responsibility: Managing Director, Human Resources & Administration

Continued on next page

5. Observations and Recommendations, Continued

Observation 4

Business Continuity Planning (BCP)

The SAS Service catalogue aligns with the Policy on Government Security and its associated BCP standard that specifies that the SAS DSO has overall responsibility for business continuity planning at OSFI.

Specifically it states:

2.1.1 OSFI Business Continuity Planning (BCP)

> *Develop and maintain the documents, plans, and practices to facilitate OSFI's response to disruptive events in order to minimize the impact to its essential services. Liaising with various stakeholders, such as IM/IT, in developing appropriate recovery strategies is an integral part of this process.*

It was observed that SAS has not fully assumed its oversight role in business continuity, as required.

- SAS did not have sufficient communication channels in place to be fully aware of the activities taken on by stakeholders, such as Information Technology Services (ITS) who manage the disaster recovery and backup processes.
- Some of the business BCP related documents used by SAS were out of date and incomplete.

Throughout OSFI, business stakeholders had processes in place to update their business continuity plans and conduct call tree tests, however without fulsome oversight the integration of the various activities cannot be assured.

Recommendation:

SAS, in its oversight role of BCP, should ensure key documents are maintained and current. Mechanisms should be developed to keep the DSO informed and knowledgeable of the key IM/IT business continuity activities occurring including the IT Disaster Recovery Plan (DRP) testing and data backup recovery processes. Formal communication channels should be developed to support the BCP coordinator/DSO in its oversight role.

Continued on next page

5. Observations and Recommendations, Continued

Observation 4

Business Continuity Planning (BCP) (continued)

Action Plan:

Management understands and agrees with the recommendations for improving the oversight role for BCP in line with our responsibilities to exercise the second level of accountability, or defense, for this subject matter area. SAS conducted an operational level Table Top Exercise in October 2013 and feedback from this was shared with EC in December 2013.

In addition, SAS is continuing to collaborate with business stakeholders and IM/IT to improve the coordination of key IM/IT business continuity activities, including the IT Disaster Recovery Plan (DRP) testing and recovery processes. and will implement more formalized processes and communications on BCP across the Office by June 2014.

Expected Completion Date: June 2014
Responsibility: Managing Director, Human Resources & Administration

Observation 5

Information Management

SAS did not always appropriately manage their information records of business value. OSFI has an enterprise electronic document management system that supports information management. SAS had many electronic records stored in the personal, shared or e-mail folders of SAS employees, which could make it difficult to retrieve and share the information in a timely manner. Internal Audit information requests in support of the audit were not always fulfilled because of SAS's process for storing documents and records of security work completed.

SAS was one of the OSFI divisions that participated in the corporate initiative to install eSpace, a SharePoint application, to replace the current enterprise Electronic Documents Management System (EDMS). The eSpace project is working on the lessons learned from the pilot participants and improvements in functionality are expected. SAS information records not on EDMS were not in the scope of the eSpace project; hence they were not moved to eSpace. SAS continues to store files outside of eSpace / EDMS exacerbating future efforts to manage information appropriately.

Inefficiencies in work processes and improper decisions may be made, and corporate memory could be impacted.

Continued on next page

5. Observations and Recommendations, Continued

Observation 5

Information Management (Continued)

Recommendation:

All SAS information resources of business value should be appropriately managed within the approved corporate repository in accordance with established Information Management practices to ensure accessibility and appropriate lifecycle management. They should not be stored in personal shared drives or email folders.

Action Plan:

Management agrees with the recommendation. Accordingly, SAS will ensure that information resources of business value are appropriately managed in accordance with the guidance and expectations of the IM group.

SAS has undertaken an exercise to review information which had been stored outside of the approved corporate repository (i.e. – eSpace) to identify information resources of business value and has moved these from personal shared drives or email folders to the corporate repository. During the transition period, information which was stored locally by SAS personnel continued to be backed up manually.

Expected Completion Date: March 2014
Responsibility: Managing Director, Human Resources & Administration

Appendix I: Audit Evaluation Criteria

Security and Administrative Services - Audit Evaluation Criteria	
Element	**Criteria**
Risk Management	▪ *External and internal risks* related to the Security function are identified, assessed, mitigation and controls are in place ▪ A *structure* exists for monitoring and managing risks and issues ▪ Management has *communicated its views and decisions* related to risk tolerance, mitigation and controls
Governance	
Operating Environment	▪ *Roles, accountabilities, responsibilities of SAS and its stakeholders* are defined and communicated to management and staff ▪ *Resources* for Security and supporting groups (e.g. IM/IT and Administration, Human Resources and Contracting) are provided for OSFI's security requirements ▪ *Technical and competencies*, including formal and informal training necessary to maintain knowledge levels and expertise are set out ▪ Security reflects OSFI's *values and a commitment related to security*
Objective Setting	▪ Security *objectives, plan and priorities (OS1) are:* o Defined and communicated to management and staff o Align with and support OSFI's plan and priorities o Align with Government policies, directives, standards and guidance
Information and Communication	▪ *Security information and performance requirements* are defined and incorporated into Security and Corporate Services reporting ▪ *Awareness on Security* is set out and communicated to management and staff ▪ *Open and timely channels of communication* exist with the Superintendent, executive, senior management, support groups and staff across the Office ▪ A C*orporate Memory* is incorporated into Security processes and maintained
Monitoring and Management Reporting	▪ *Management reporting* is in place to monitor Security plans and priorities as well as the Office's overall security ▪ *A continuous improvement process* exists to monitor and report on: o Achieving Security objectives, plan and priorities o Adherence to security policy, processes and practices (non-compliance) o Areas for improvement o Adequacy of resources to support security in the Office
Control Process	
Process and Control Activities	▪ A *management oversight* process exists over Security ▪ *Process for* reviewing Office security practices that incorporates an assessment of the risk, control, residual risk and impact at the corporate, sector and division level ▪ *Back-up and continuity plans* of the Security function and staff are in place