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 Information Management / Information Technology (IM/IT) - Governance

November 2012

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 Information Management / Information Technology (*IM/IT*) Governance was approved by the OSFI Audit Committee and the Superintendent for inclusion in the OSFI 2011 to 2012 Internal Audit Plan.

This report presents the results of that audit based on audit work completed at the end of July 2012. The audit recommendation will support the IM/IT Division with its approach to governance.

This report was presented to the OSFI Audit Committee and approved by the Superintendent on November 23, 2012. The Assistant Superintendent, Corporate Services, and the Chief Information Officer, who have provided their management comments within this report, have also reviewed it.

Context

Overview – Why this is important

In knowledge-based institutions such as OSFI, organizational success is dependent on the data or information that is provided and sustained by technology being secure, accurate, reliable and available to Management and staff when needed. IM/IT Governance is the responsibility of Executive Management and is an integral part of enterprise governance. It consists of the leadership and organizational structures and processes that ensure that the organization's IM/IT achieves, sustains and extends the organization's strategy, objectives and operational business services' efficiency and effectiveness.

The appropriate IM/IT Governance and stewardship are needed to ensure that the investments in IM/IT will generate the required business value and that the risks associated with IM/IT are identified, understood and mitigated.

Overview of OSFI's IM/IT Governance

The activities of the IM/IT Division support OSFI's mandate by maintaining and operating an IM/IT infrastructure to support the Business' operations effectively; to minimize downtime; and to facilitate the storage of all electronic information. The IM/IT Division also establishes and maintains an operationally secure network environment to safeguard electronic information, in accordance with the TBS' *Policy on Government Security* and its related Standards.

Continued on next page

1. Background, Continued

Overview of OSFI's IM/IT Governance (Continued)

OSFI has a number of legacy systems that require increasing maintenance. These legacy systems are being replaced, consolidated, improved, maintained or contained as part of OSFI's Information Technology Renewal (*ITR*) program.

The ITR program, (a five year technology transformation), was initiated to equip OSFI with renewed business capabilities. OSFI's IM/IT Strategy was approved by the Executives in June 2009 and was shortly followed by internal work realignment and organizational redesign to position the IM/IT division to deliver the renewal work. New IM/IT governance was also established to manage the change and to make the required decisions throughout the program. The ITR program commenced in 2010/11 and is one of OSFI's largest annual expenditures.

Objectives of the IM/IT Division and OSFI's strategic priorities

The objectives of the IM/IT Division are:

- To maintain and operate OSFI's information technology infrastructure and services in support of OSFI's operations, minimizing downtime and facilitating the storage of, and access to, OSFI's information assets in a cost-effective manner.
- To conduct and support the evolution of OSFI's information systems to meet changing needs and to keep pace with technological change.
- To establish and maintain a secure network environment to safeguard OSFI's information holdings in accordance with established Government policy and the sensitivity of the information.
- To maintain and support secure, flexible and reliable information systems and their associated environments in order to enable OSFI employees to effectively create, collect, store, use, protect and share the information required to meet their business commitments.
- To work with other Sectors / groups across OSFI on a collaborative basis to deliver all new and modifications / upgrades to user applications, large and small, in a timely and effective manner, and in accordance with the Treasury Board Secretariat's (TBS') policies, as applicable.

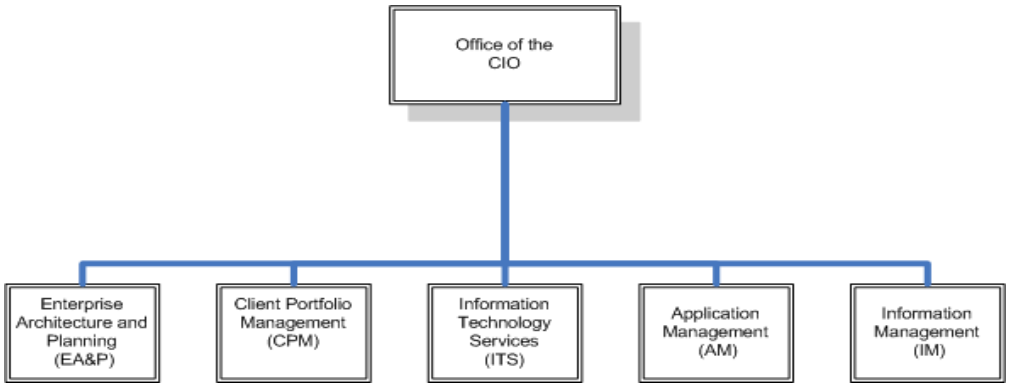
An enhanced corporate infrastructure is one of the four strategic priorities, or OSFI-wide areas of focus over 2012 – 2015, which support OSFI in meeting its mandate; mitigating its risks; and achieving its strategic outcomes. The IM/IT Division supports this strategic priority by continuing to champion the Information Technology Renewal (*ITR*) program to achieve targeted milestones as it shifts focus from the implementation of OSFI common tools and services to business application renewal.

Continued on next page

1. Background, Continued

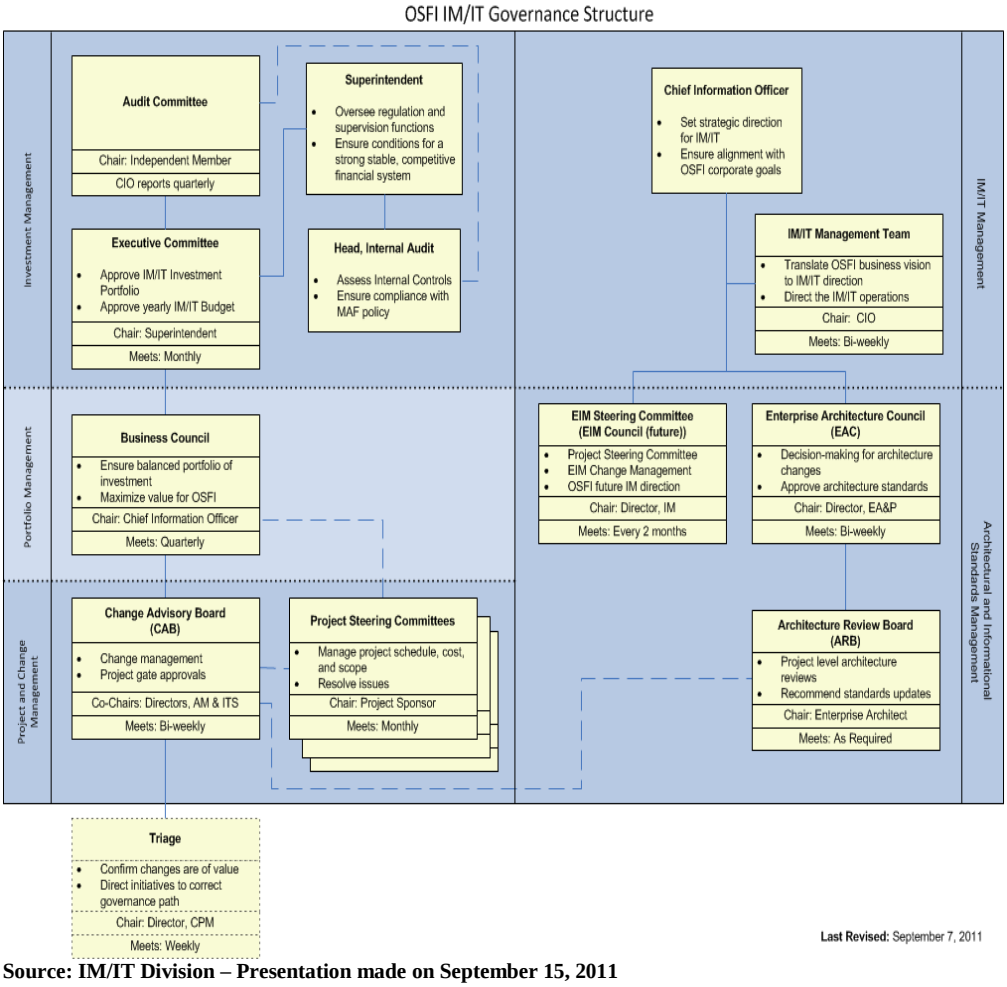
OSFI's IM/IT Organization

The IM/IT Division is part of the Corporate Services Sector that is led by the Assistant Superintendent, Corporate Services. The Chief Information Officer (*CIO*) is responsible for the IM/IT Division, which consists of approximately 80 full-time staff and consultants within the following five groups:



OSFI's IM/IT Governance structure

OSFI's IM/IT Governance structure is an integral part of OSFI's enterprise governance comprised of the following:



Source: IM/IT Division – Presentation made on September 15, 2011

Continued on next page

1. Background, Continued

Overview of the Policy Framework

OSFI has a number of IM/IT policies and procedures in place to support the overall IM/IT Governance. These policies and procedures are largely derived from the Treasury Board Secretariat's (*TBS'*) frameworks, directives and policies that are applicable for IM/IT Governance at OSFI. Please refer to ***Appendix 1: Reference list of TBS' policies and other industry best practices.***

OSFI has also implemented various security policies and procedures to address government requirements, known risks and best practices. The Departmental Security Plan (*DSP*) that is required by the TBS' *Directive on Departmental Security Management*, will be the principal vehicle for identifying new/ additional risks and the recommended actions to mitigate them, including additional policies and procedures to support the ITR program. The draft DSP has been completed and is yet to be presented to the Executives for their review and approval. One of the requirements of the TBS' *Directive on Departmental Security Management* is for all departments to implement a DSP by June 30, 2012.

2. Audit Objective, Scope and Approach

Audit Objective

The objective of the audit is to provide reasonable assurance that OSFI has an appropriate Information Management / Information Technology (*IM/IT*) Governance structure and related monitoring controls in place, by assessing that:

1. An appropriate IM/IT organization structure exists with clear roles and responsibilities for the IM/IT functions, including security; IM/IT decision-making; and IM/IT investments.
2. The IM/IT Strategic Plan is aligned with the Corporate Strategic Business Plans and Priorities.
3. IM/IT investment planning supports the corporate strategy.
4. IM/IT strategic planning follows a structured approach that is managed and measurable.
5. IM/IT investment budgeting and expenditures are appropriately monitored.

Continued on next page

2. Audit Objective, Scope and Approach, Continued

Audit Scope

The scope of the audit is for the period April 01, 2011 to March 31, 2012. It included a review of:

- The IM/IT organization structure and key functions underlying and supporting the IM/IT Division in the execution of their mandate, which were in place during the period.
- The IM/IT strategic plan/ IT Renewal program and their alignment with the corporate strategic business plans and priorities.
- Management's monitoring of its IM/IT performance metrics, including costs.

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's *Policy on Internal Audit*.

The IM/IT Governance audit was predominantly conducted by leveraging the internationally recognized Enterprise Risk Management – Integrated Framework recommended by the Committee of Sponsoring Organizations of the Treadway Commission (*COSO*), using a subset of the ISACA COBIT 4.1 control objectives that are linked to ITIL V3 Best Practices supporting information.

Internal Audit also leveraged from:

- the Treasury Board Secretariat's (*TBS'*) frameworks, directives and policies that are applicable for IM/IT Governance at OSFI; and
- other IM/IT Governance industry standards, best practices or control frameworks, as appropriate during the audit.

Please refer to ***Appendix 1: Reference list of TBS' policies and other industry best practices***.

The approach to conducting the audit included:

- review of relevant documentation, such as the applicable TBS and internal policies and procedures, organization charts, roles and responsibilities, agendas and minutes of meetings, investment plans, strategic plans and priorities;
- direct observations of a number of key IM/IT Governance committee meetings;
- walkthroughs of the main supporting IM/IT processes; and
- discussions/ interviews with key personnel and stakeholders.

Continued on next page

3. Conclusion

Conclusion

Management has an appropriate Information Management / Information Technology (*IM/IT*) Governance structure and processes in place that are comparable with the best practices of similar federal departments and agencies.

OSFI's IM/IT Division has established a strong foundation for IM/IT governance with continued learning and enabling capabilities. As OSFI's IM/IT Governance continues in its maturity journey, it is well positioned to leverage this solid foundation to further enhance OSFI's assessment of the privacy and information security requirements for its applications and data.

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 opinion 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 evidence was gathered in compliance with Treasury Board policy, directives and standards on internal audit, and the procedures used meet the professional standards of the Institute of Internal Auditors. The evidence has been gathered to be sufficient to provide senior management with the proof of the opinion derived from the internal audit.

We wish to recognize the excellent rapport and exchange of views with all involved in the audit. The depth of the review and focusing on what matters would not have been possible without the support received throughout the audit.

_____ _____

Chief Audit Executive, IA Date

4. Observations and Recommendations

An appropriate IM / IT organization structure exists

a. An IM/IT Governance framework exists for decision-making, direction, and accountability. OSFI's IM/IT Governance framework is consistent with the best practices found in some of the other similar-sized federal departments and agencies.

b. Key strategic and tactical IM/IT Governance Committees exist with effective terms of reference; clear mandates and reporting structures; appropriate memberships; and defined roles and responsibilities.

c. The IM/IT organizational structure is appropriate for the size and nature of OSFI, with defined roles and responsibilities for the IM/IT functions, authorities and reporting structure.

d. Key IM/IT operational committees have the appropriate representation by senior management from the business; from the IM/IT division; and from the Security and Administrative Services (*SAS*) group.

e. The Chief Information Officer provides regular reports to the Executives and to the Audit Committee.

f. The CIO has Executive Management's support for the authority and resources to execute the IM/IT Strategic Plan.

The IM/IT Strategic Plan is aligned with the Corporate Strategic Plan

a. The IM/IT strategic plan is aligned to OSFI's strategic direction and incorporates the key business requirements and strategic priorities.

b. The business provides the IM/IT division with direction and support relating to investment decisions that the division incorporates into its IM/IT Strategic Plan.

IM/IT investment planning supports the corporate strategy

a. IM/IT's investment planning supports the corporate strategy and is consistent with the best practices found in some of the larger-sized federal departments and agencies.

b. Objectives for the IM/IT strategic and investment planning activities are defined; are aligned with and support the corporate strategic plans and priorities; are prioritized; and are communicated to the appropriate stakeholders.

IM/IT strategic planning follows a structured approach

a. OSFI has a defined IM/IT Strategic Planning process with appropriate decision-making and control points.

b. The policies, practices and procedures for the strategic planning and the investment planning processes are communicated to the appropriate stakeholders.

c. Objectives for the IM/IT strategic and investment planning activities are communicated to the appropriate stakeholders.

Continued on next page

4. Observations and Recommendations, Continued

IM/IT investments are monitored

a. OSFI has an effective governance process for preparing, assessing and monitoring business cases to assess IT investments based on a balance of risks, costs and benefits.

b. IM/IT's management of the Information Technology Renewal (*ITR*) program is consistent with the practices found in some of the other similar-sized federal departments and agencies.

c. Appropriate management reporting practices are in place to monitor progress against the plan.

d. Executive oversight exists over the execution of the IM/IT Strategic Plan.

Observation #1:

Opportunity to enhance the IM/IT strategy and risk management approach

As OSFI's Information Technology Renewal (*ITR*) program progresses, the IM/IT Division can further enhance its strategy and risk management approach by developing and implementing, in collaboration with the Departmental Security Officer (*DSO*), a cost-effective plan for an ongoing risk assessment of OSFI's applications and data, to ensure that they continue to meet the appropriate security and privacy requirements.

OSFI last performed an Enterprise IM/IT "Threat Risk Assessment" (*TRA*) for its applications in 2007. However, the ongoing ITR is changing some of the common components of OSFI's overall IM/IT infrastructure. Although OSFI performs some form of risk assessment when moving a change through the various stages of an application's development life cycle and into Production (via the review and approval process of the Triage Committee and the Change Advisory Board (*CAB*)):

- there are no mandatory requirements for performing a privacy, IM or IT security risk assessment; and
- there appears to be no systematic cost-effective approach for periodic risk assessments of its IM/IT applications and data going forward, to ensure that they continue to meet the appropriate security and privacy requirements.

Recommendation #1

To be consistent with both the best practices of some of the other federal departments and agencies and with the guidance from the applicable TBS policies and standards, OSFI should develop and implement an approach to require privacy and security risk assessments of its IM/IT applications and data, to ensure that they meet the appropriate security and privacy requirements.

Continued on next page

4. Observations and Recommendations, Continued

Recommendation #1 (Continued)

To obtain cost-efficiencies, OSFI need only capture these requirements in a central repository, then leverage from this repository to perform a risk assessment on the common IM/IT components. Any residual risks to the applications/ data are then assessed by the Change Advisory Board (*CAB*), in conjunction with the business owners.

Such an approach should include a review and update of the Change Management policy to ensure that the checklists for the Change Advisory Board (*CAB*) and the various supporting committees are adjusted accordingly to require that privacy, IM and IT security risks are assessed and formally agreed with the business, before promotion to Production.

5. Management Response and Action Plan

Overview

This report has been reviewed by the Chief Information Officer (*CIO*) and the Assistant Superintendent, Corporate Services, who acknowledge its observation and recommendation.

The audit recommendation will support the IM/IT Division with its approach to governance.

Management Responses / Comments

Management agrees with the recommendation of this audit. The following background is relevant to the recommendation and IM/IT's ability to act upon it:

In 2009, as a result of the 2007 "Threat Risk Assessment" (*TRA*), OSFI completed a security classification exercise and consequently understands its information holdings. Approximately 90% of the information OSFI holds is designated "business confidential" which, for the Government of Canada (*GoC*), is security classified as Protected "B" in accordance with the TBS' *Policy on Government Security*. The Office also holds personal information which is either Protected "A" or "B". This personal information must be specifically defined by a Privacy Impact Assessment before it is collected, and then protected and retained in one or more Personal Information Banks, once received. There is virtually no Protected "C" information in OSFI's information holdings. Therefore, OSFI has a relatively homogeneous and well understood set of information from a privacy and security perspective.

In 2011-12, as a part of IM/IT's on-going lifecycle maintenance program, several "end of life" data network components were replaced, and at the same time the network structure was redesigned to meet Government of Canada

Continued on next page

5. Management Response and Action Plan, Continued

Management Responses / Comments (Continued)

(*GoC*) best practices, such as the Management of Information Technology Security (*MITS*) standards. As a result, OSFI's network core is secure and fully ready to meet the recommendation of this audit.

Implementation details are outlined in the Management Action Plans section.

Management's Action Plan

In response to the recommendation of this audit, IM/IT in collaboration with OSFI's Security and Administrative Services, will make changes to existing policies, procedures and the affected system (*ITSM*), in order to create and maintain an inventory of applications and data, including the associated information security/privacy risks. Business owners will be made aware of and educated about these issues as they affect them, and reports will be available in ITSM to monitor progress. The actions will be completed by the end of FY 2013-14.

Appendix 1: Reference list of TBS' policies and other industry best practices

Reference list of TBS' policies

The following provides a list of the Treasury Board Secretariat's (*TBS*) frameworks, directives, policies and standards that are applicable for IM/IT Governance at OSFI:

- Treasury Board Secretariat's (*TBS*) Management Accountability Framework (*MAF*)
- TBS Policy Framework for Information and Technology
- Policy on Information Management
- Policy on Management of Information Technology
- Directive on Management of Information Technology
- Policy on Investment Planning – Assets and Acquired Services
- Policy on Government Security
- Directive on Departmental Security Management
- Operational Security Standard: Management of Information Technology Security (*MITS*)

Reference list of industry best practices

The following provides a list of Industry Standards, Best Practices and Control Frameworks:

Name	Category	URL
ISACA ValIT	IT Governance Framework	http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Val-IT-Framework-2.0.aspx
ISACA COBIT	IM/IT Control Framework	http://www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx
ITIL – Information Technology Information Library	Best Practices	http://www.itil-officialsite.com/
PMI PMBoK – Project Management Body of Knowledge	Project Management Standards	http://www.pmi.org/PMBOK-Guide-and-Standards.aspx
TBS - Enhanced Management Framework	Treasury Board Best Practice	http://www.tbs-sct.gc.ca/emf-cag/index-eng.asp

---