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

Internal Audit Report on IT Security Access

January 2010

OSFI BSIF

Canada

Contents

Background

Introduction

An assessment of the framework under which OSFI's IT security infrastructure & related applications/systems and controlled/restricted access to OSFI's electronic information (*IT Security Access*) is provided and the degree to which the framework is being applied was approved by the Audit Committee and the Superintendent for inclusion in OSFI's 2009-10 Internal Audit Plan.

In preparing the audit plan, we reviewed security policy, guidance and practices with an emphasis on access to and protection of electronic information and related practices, measures and tools[1]. As well, we met with the Assistant Superintendent, Corporate Services, and the Directors of Security and of Infrastructure Technology Services, Information Management/Information Technology (IM/IT) division.

OSFI has a comprehensive IT security architecture as illustrated in *Diagram 1- IT Security Architecture* providing restricted access to OSFI's electronic information on a need-to know basis. The IT security architecture has two distinct 'security zones': Public, Corporate Network, Recovery Cold Site and Offsite Tape Storage.

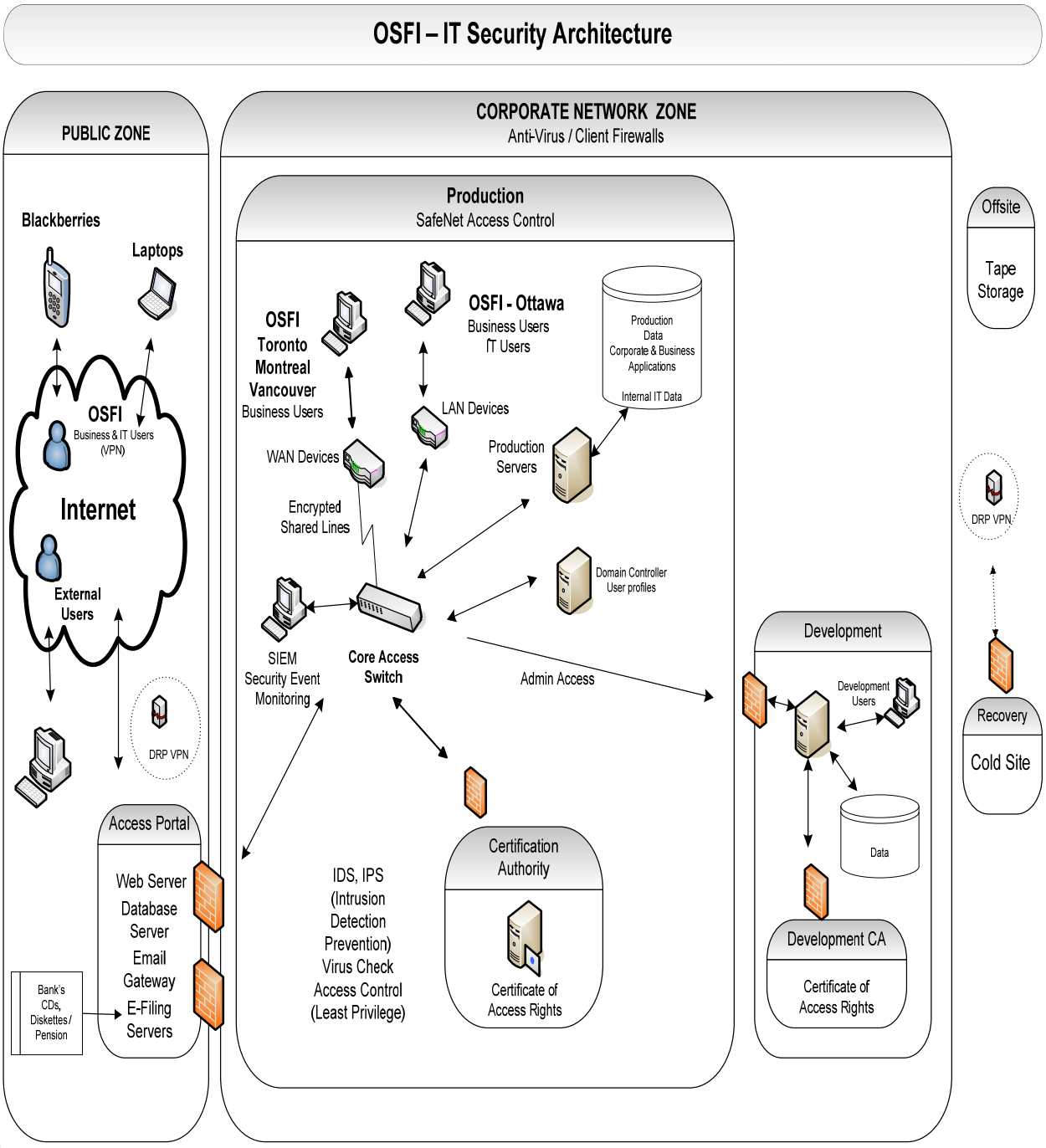
The *Public Zone* is outside OSFI's Corporate Network services. Through the Internet, employees[2] gain access to OSFI's network using laptops, blackberries and PCs. Public Zone services include access to OSFI's public website and related databases, and remote access to electronic filing, external e-mail and Corporate Network services.

Security measures employed include two factor authentication (smart card), firewalls, intrusion detection prevention, dynamic monitoring and Virtual Private Network devices (VPN services use specialized hardware to build a private network capability over existing public network lines). VPN devices allow for a secure connection between two IT environments - workstation to server or server to server - by encrypting all traffic (data) over that connection.

The *Corporate Network Zone* has two *domains*, one each for production and development. Employees in OSFI's offices gain access to Corporate Network services through LAN and WAN encrypted lines. Security measures employed include two factor authentication (smart card), Virtual Private Network (VPN) devices, firewalls, certification authority and controller user profiles, other administrative practices, and security event monitoring.

[1] TBS Operational Security Standard: Management of Information Technology Security (MITS); TBS Policy on Government Security (PGS); Control Objectives for Information and related Technology (COBIT)
[2] Including security cleared non-employees

IT Security Architecture ***Diagram 1***



Terms used

AEG	Advisory & Evaluation Group, part of IM/IT change management process
CMP	Change Management Process, IM/IT process for managing user requests for change. The CMP includes the CAB and AEG groups
CAB	Change Advisory Board, part of IM/IT change management process
CIO	Chief Information Officer, IM/IT
COBIT	Control Objectives for Information and related Technology (IT governance and management control framework)
COSO	Committee Of Sponsoring Organizations of Treadway Commission framework (control framework)
PGS	TBS Policy on Government Security
IM/IT	Information Management/Information Technology division
IT based assets	Business applications, IT infrastructure and related hardware & software, personal IT devices such as Blackberries, etc. Also, refer to Diagram 1, page 4
IT security based assets	SafeNet (smart card) security measure, the IT security architecture design, etc. Also, refer to Diagram 2, page 9
ITIL	Information Technology Infrastructure Library, UK (de facto standards, best practices for IT service management)
ITS	Infrastructure Technology Services, the IT operations group in IM/IT
LAN	Local Area Network
MITS	TBS Operational Security Standard: Management of Information Technology Security
PMG	Project Management Group, the systems development group in IM/IT
RACI	A roles and Responsibilities model: **R**esponsible for task**, A**ccountable, **C**onsulted & **I**nformed persons
SafeNet	Smart card technology/software to provides restricted access to PCs and electronic information through a specific and controlled User identification and password
IT Security Access Framework	Security and ITS policy, guidance, processes / activities and measures / tools associated with access to and protection of OSFI's electronic information.
SSU	Security Services Unit, the security group in OSFI
TRA	Threat and Risk Assessment
Users (Applications)	Supervision, Regulation and Corporate Services Sectors, Pensions Division and Office of the Actuary (applications)
VPN	Virtual Private Network
WAN	Wide Area Network

Providing assurance

In order to manage its work in a complex and rapidly changing environment, OSFI develops and puts in place specialized policies, guidance and processes. In general, these are called internal control frameworks. These frameworks provide assurance to the Superintendent and senior management that the nature and scope of work required to carry out OSFI's mandate is well defined and that consistency and quality of the work is maintained.

Such management frameworks and their application are essential to the Superintendent and the Audit Committee to enable them to fulfil their responsibilities under the Treasury Board Policy for Internal Audit regarding OSFI's governance, risk and control processes. Under the Policy, Audit & Consulting Services is to conduct assurance audits of OSFI's operations and supporting corporate services reporting on how well they are designed (internal control framework design) and how they are working (the application of the frameworks in meeting business objectives).

Audit objectives

The objectives are:

- To provide an assessment of the *internal control framework* (*IT Security Access*) under which OSFI's security and IT security infrastructure provides restricted access to and protection of its electronic information
- To provide an assessment on how well and the degree to which the *smart card (SafeNet) security measure* is being applied
- Identify *potential areas for improvement*, as appropriate

Audit scope

The audit covers the *IT Security Access* internal control framework (Security and ITS policies, guidance, processes and practices associated with restricted access to and protection of OSFI's electronic information) for the 2009-10 fiscal period *as at December 2009* as well as any improvements underway in the 3rd Quarter 2009-10 and planned looking forward. The work will include testing use of the SafeNet security measure, during the period from *1st Qtr to end of 2nd Qtr ending September 2009.*

Matters *outside of the scope* of this review are:

- An assessment of the degree to which IT security access measures are applied in the Office, *except* for a walkthrough of existing and planned structures, activities, processes and tools associated with IT security access and detailed testing of network security as noted above.
- A review of OSFI's infrastructure technology architecture *except* as it is related to the IT security architecture
- A review of application/system development practices *except* as they are related to administration of IT security restricted access to the development environment.
- A review of non-IT safeguards such as premises and facilities, information classification, and employee and contractor security screening

Audit approach

The audit was conducted according to 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 was conducted to provide high assurance on the audit findings, analysis, and observations, and recommendations.

The *IT security access* audit work included:

- A review and walkthrough of existing, underway and planned structures, activities, processes and measures/tools as they are related to the *design of the IT security access internal control framework* including security monitoring, analysis, assessment and reporting including outsourced network perimeter monitoring and incident response
- A review and walkthrough of the *IT security architecture* and related structures, activities, processes and measures/tools
- A review and a walkthrough of existing, underway and planned structures, activities, processes and measures/tools as they are related to *use of SafeNet* across the Office and testing of employees' use of SafeNet in carrying out their work. A representative sample of 20 to 40 business and IT users will be selected for reviewing the *use of SafeNet*
- Interviews with *Security Services Unit and ITS management and staff as well as a selection of business and IT user of OSFI's IT services*.
- An *identification and application of comparable practices and methodologies* associated with *IT security access* to and protection of electronic information including MITS, PGS, ITIL, Project Management Institute - Project Management Book of Knowledge, and information and assessments available through leading associations such as ISACA

Internal control framework

The IT secure access internal control framework (criteria elements and related components) as set out in *Appendix A- Internal Control Framework* was used as the basis for assessing IT secure access internal control policy, guidance, processes/activities and measures/tools.

The criteria were developed from varied sources of security and IT security policy and guidance, and best practices[3] in consultation with the Director of Security, the CIO and Director of Infrastructure Technology Services, IM/IT. The scope and complexity of OSFI's IT environment and its information as well as related inherent risks were considered in developing the internal control criteria.

The internal control criteria were accepted by the Assistant Superintendent, Corporate Services, as the basis for assessing and reporting on IT security access to electronic information.

[3] These criteria are drawn from and aligned with the control frameworks: COSO (COmmittee of Sponsoring Organizations of Treadway Commission, MITS (TBS Operational Security Standard: Management of Information Technology Security), and COBIT (Control OBjectives for Information and related Technology).

Observations, Assessment and Recommendations

Overview

Our audit covered the *IT Security Access internal control* framework *as at December 2009* and improvements implemented and underway in the 3rd Quarter 2009-10 and forward, and a review of the application the *SafeNet smart card* security measure (restricted access to IT information) for the period *from April 2009 to the end of September 2009.*

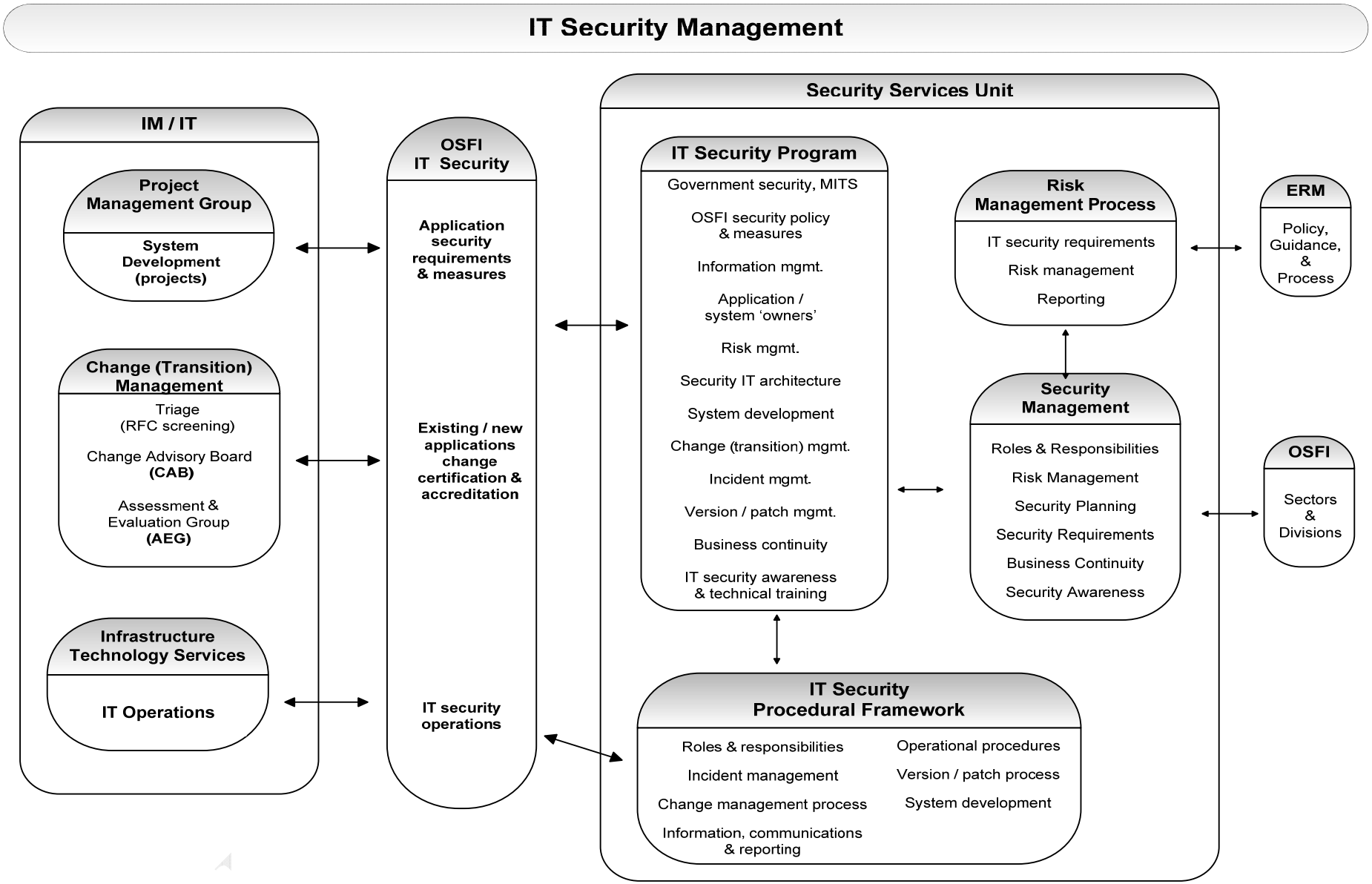
The audit work was conducted on a collaborative basis as security and IT improvements were implemented and underway while conducting the audit work. There were ongoing discussions with the Director of Security Services and Director of Infrastructure Technology Services, IM/IT and key staff maintaining and providing security and IT security services.

We observed and examined all components of the *IT Security Access* internal control framework. We found that OSFI has a robust IT security architecture, *Diagram 1 - IT Security Architecture.* To follow the audit observations, assessment and recommendations refer to *Diagram 2 – IT Security Management* that illustrates the interaction of the Security Services Group with key groups in the Office as well as the frameworks/activities involved in managing IT security. As appropriate, we recognized the number of improvements implemented and undertaken during our audit. These actions will require a focused co-ordinated effort between Security Services Unit and IM/IT, business and functional managers and management.

Although we found key components of an effective *internal control framework*, we identified other areas where key improvements in the internal control framework for IT security are needed Our comments and recommendations focus on:

- Formalizing and strengthening IT security policies and procedures into an overarching IT security program
- Establishing a security risk management process at an operational level
- Strengthening the IT security procedural framework between Security Services Unit, and Infrastructure Technology Services and other IM/IT groups

IT Security Management *Diagram 2*



Internal Control Elements/Components	Observations, Assessment and Recommendations

Governance: Objective setting & operating environment

- *Oversight accountabilities exist*
- *Roles and responsibilities are defined, communicated and understood*
- *IT security access policy and practices are fully developed*

Recommendation
Formalize and strengthen IT security policies and procedures into an overarching security program incorporating the Policy on Government Security with MITS standards, guidance and practice requirements

The Security Services Unit (**SSU**) and Infrastructure Technology Services (**ITS**) groups manage and provide IT security services across the Office. Following the Policy on Government Security (**PGS**) and the Management of Information Technology Security (**MITS**) guidance, respective IT security roles and responsibilities have been established using a RACI[1] *accountability* model consistent with PGS and MITS guidance as appropriate to OSFI's IT environment. Based on the RACI analysis, the respective groups are putting in place *operational* policy, guidance and processes on a priority basis to integrate and co-ordinate IT security work.

*Note 1: RACI: **R**esponsible for task, **A**ccountable, **C**onsulted & **I**nformed persons. A RACI matrix is a type of responsibility assignment tool showing the relationship between activities and staff members. The full description of this tool can be found under Organization Charts and Position Descriptions in the PMBOK (fourth edition) – Develop Human Resource Plan process.*

As a core member of the Change Advisory Board (**CAB**) and the Assessment and Evaluation Group (**AEG**) SSU is an integral part of IM/IT's change (transition) management process (**CMP**). A key CMP role is managing the assessment and routing requests for change (**RFC**) to the appropriate change/development process - a minor standard change, a significant change, a system development project or an IT operational project. System development and IT operational project RFCs are managed by separate processes. SSU is a signature member of system development projects with respect to security and IT security matters. The CPM should advise the SSU of IT operational projects such that security involvement can be determined as appropriate.

An earlier external review of security governance within the Office recommended the establishment of a *security management forum*. SSU indicated that forming such a forum is under review. We strongly support this initiative. A forum provides input to the adaption of PGS and MITS requirements to OSFI's environment, the design of the corporate security program including business application security requirements and measures, and the development of corporate-wide security plans.

Soon to be released TBS security planning guidance calls for the development, implementation and maintenance of departmental (OSFI) security plans that 'details decisions for managing security risks and outlines strategies, goals, objectives, priorities and timelines for improving departmental security'. It is important that all stakeholders, Sectors/Division, are directly involved in the development and maintenance of security (and IT security) policy, guidance, and security programs.

Current security documents include elements of policy, standards and procedures but are not always complete. For example, an internal policy gap analysis highlighted the need for policy and guidance in areas of asset management, vulnerability/incident management, application security standards, and disaster recovery planning. Security policy and guidance exists and is communicated in the Office. There is not an overarching security (and IT security) program that ties together PGS, MITS and internal security needs into an integrated and comprehensive set of policies, guidance, processes and tools. Without such an overall structure, it would be difficult to know whether ongoing activities as described above will carried out in a coordinated and consolidated fashion.

Internal Control Elements/Components	Observations, Assessment and Recommendations
	We recommend that the Office, on a priority basis, formalize and strengthen IT security policies and procedures into an overarching security program incorporating the Policy on Government Security with MITS standards, guidance and practice requirements as adapted to OSFI's IT environment.
Risk Management	
▪ *Risk and risk tolerance is consistent with the ERM practices* ▪ *Determination of IT security requirements are based on the assessment of the IT environment* ▪ *IT security risks are identified, assessed and mitigation controls are implemented*	OSFI's Enterprise Risk Management policy and processes are used for the identification, assessment and mitigation of potential risk at the Sector and Group levels. At the Corporate Services Sector level security and IT security risks are identified, evaluated, and, as appropriate, incorporated into ERM action plans. Security related risks are incorporated into OSFI's ERM risk assessments. There is not a specific security risk management process for the identification, assessment, mitigation and management of operational security and IT security risks. A security risk management process, shaped by PGS and MITS and aligned with ERM, is essential so that security requirements and potential IT risks are identified, assessed and reported on a consolidated basis to ERM and management. Such a risk management process would be aligned with key IM/IT functions and processes such as portfolio management, system development, IT operations, application / system release, and incident and version/ patch update management.
Recommendation Establish a security risk management process at an operational level that incorporates IT security requirements, identification & assessment of IT security risk, security risk management and reporting consistent with ERM practices	SSU conducts regular IT security risk assessments (vulnerability assessments, threat/risk assessments) as well as independent IT security threat and risk Assessments (TRAs) with reporting to management on key issues and concerns. The results of such assessments are assessed in respect of the impact on OSFI and actions/recommendations are proposed. Actions are prioritized and resources are identified. In addition, ITS conducts ongoing monitoring of the external and internal environments, and performs daily vulnerability and risk assessments. The process for sharing the results of these assessments should be formalized. SSU makes queries of and does follow up on SSU assessments and ITS IT operations risk assessments such as potential denial of service and penetration attacks. There is not a process for inventorying, tracking and reporting to determine whether these security issues/concerns have been addressed. Such a process for follow up on IT security assessments/recommendations is essential to maintaining OSFI's IT security environment. According to recent IT security assessments, external risks are controlled by stringent perimeter controls. However, internal IT security monitoring processes are less robust. There are informal processes and inconsistent practices related to version/security patch, vulnerability and incident management. ITS has begun the process of implementing security patches at the IT operating system level. Along with our recommendation that OSFI formalize and strengthen IT security policies and procedures into an overarching security program under Governance and Accountability section, we recommend that SSU establish an operational *security risk management process* to shape IT risk management and underlying security and IT security policy and measures as key input into an IT security program. The security risk management process would provide valuable information and assessments of IT security risk for input in setting overall OSFI's risk tolerance, design of OSFI's IT security environment, and design of business applications security policy and measures.

Internal Control Elements/Components	Observations, Assessment and Recommendations
	We recommend establishing a security risk management process at the operational level that incorporates IT security requirements, identification & assessment of IT security risk, security risk management and reporting consistent with ERM practices.
Control Processes	
▪ *Security planning & resources incorporate IT security requirements* ▪ *Establish a security protection program that includes IT security measures* ▪ *There is incident management* ▪ *System development & change management incorporates IT security requirements* ▪ *Continuity / recovery planning includes IT security requirements* *Recommendation* Strengthen the IT security procedural framework to incorporate procedures for incident management, version / patch updates, technology certification and accreditation & continuity / recovery planning, and related security and resource planning	The TBS Management of IT Security standard (MITS) specifically asks departments and agencies to adopt an active defence strategy that includes prevention, detection, response and recovery. An OSFI *security protection program* exists along with a robust IT security architecture, *Diagram 1 - IT Security Architecture*. The IT security architecture provides for restricted access to electronic information through security measures including two factor authentication to OSFI's internal IT environment (corporate network), encrypted virtual private network communications, firewalls, certification authority and access privileges, as well as full laptop and PC data encryption. Active monitoring of IT risks and safeguards are in place. IT staff have two access accounts, a user account for normal administrative tasks and a separate 'supervisory / administrative' account reserved for operational tasks. OSFI has in place many of the components of a security procedural framework. However, they are informal, limited in scope, and the work of SSU and ITS is not well integrated in forming an IT security posture. For example, although the network is monitored by IT staff, security information, issues and assessments are provided to SSU on an ad hoc basis. Based on RACI, the groups are putting in place *operational* policy, guidance and underlying processes that designate IT security roles and responsibilities between the two groups. IT security assessment criteria and a process for bringing IT security issues and assessments to SSU's attention are under development in the spirit of the two groups working side by side. An anticipated new TBS policy on security planning focuses on pulling all components of security (including IT security) into an overall security plan as input to corporate planning and resource identification. Such a plan would include policy, security requirements, guidance, administrative and IT support, and employee awareness and technical training for both overall security and its component, IT security. It will be necessary to integrate security plans into business & IT plans, and operations and supporting functions. Establishing a *security risk management process* (refer to Risk Management section of the observations) and developing a security *procedural* framework are essential in enabling such a planning effort. As a member of the TBS development group, SSU has early knowledge of these requirements and is, therefore, well positioned to design and implement the new planning policy. OSFI plans to implement the new policy during 2010-11. A key component of putting in place a *security management program*, as outlined in Governance & Accountability, is knowing who owns and is responsible for IT based assets (business applications, IT infrastructure, personal IT devices such as Blackberries, etc.). As only about half of the business applications have a designated owner it is difficult to know if security policy and measures meet the business needs, and whether there is the right balance between IT risk and business needs. Lack of owner participation in security policy, IT risk tolerance, and the selection of security measures could have an impact on the design of their business applications and whether the measures are user friendly. Under the RACI initiative, SSU is now the designated owner of OSFI's IT security based

Internal Control Elements/Components	Observations, Assessment and Recommendations
	assets such as the SafeNet smart card security measure and the IT security architecture design. ITS as the owner of IT infrastructure provides technical security design support and provides IT operations services. For example, the smart card security measure is the backbone of OSFI's IT security architecture in which access to electronic information is restricted on a need-to-know basis based on two-factor authentication (a smart card: what you have and a user password: what you know). Key components of this security measure are in place. However, the individual components need to be pulled together setting out oversight and management responsibilities, policy, guidance, IT and user requirements, and employee awareness and technical training. Other essential components of a *security management program* are change management, system development and release of software into the production environment (transition management). A challenge for security is defining its role and responsibilities in transition management (release of applications/systems to the IT production environment). With SSU joining the CAB and AEG IM/IT groups (refer to Governance and Accountability section of the observations) SSU is now directly involved in discussion of security and IT security matters as they arise from a user 'request for change'. In this way, IT security requirements, risk and security requirements are identified and addressed in a pro-active posture. Although SSU is involved in review and release of new and changes to legacy applications, the IM/IT transition management process does not call for a formal review and sign-off by SSU before applications/systems are released into the production environment as part of a certification and accreditation checkpoint. This checkpoint should be incorporated into existing transition management checklists and practices. Under RACI initiative, the role of SSU in assessing the impact and priority of IT security updates (patches) has been incorporated into version/patch management. Security patches are being prioritized and implementation plans are being put in place. Business Continuity Planning (BCP) is acknowledged as a priority. Updating of both the BCP plan and the Disaster Recovery Plan (DRP) is underway. A formal, strengthened BCP process is needed to incorporate DRP planning. *We recommend strengthening the IT security procedural framework to incorporate procedures for incident management, version/patch updates, technology certification and accreditation, continuity / recovery planning, and related security and resource planning.*
Governance: Information, Communications & Reporting	
▪ *IT security access information is* ▪ *defined, gathered, assessed and incorporated into reporting* ▪ *communicated among security and stakeholders on a continuous basis* ▪ *incorporated into security awareness of employees& training*	As set out under Risk Management, SSU conducts threat and risk assessments (TRA) and ITS continuously monitors the external and internal IT environments. The information and assessments are shared on an ad hoc and informal basis. As a result, there is no routine reporting with regard to security matters or consistency of what information is communicated, to whom and when. It is essential that the right security information is reported to the right parties at the right time. Until key operational and security processes such as incident management, version/patch management and software release are fully established, IT security information will not be available for regular assessment and reporting. Reporting on IT security risks, vulnerabilities, incidents, events and mitigation actions to those who should know and take action is not assured; also it is uncertain as to whether the information will be received on a timely basis.

Internal Control Elements/Components	Observations, Assessment and Recommendations
of Security and IT staff *Recommendations* Strengthen the IT security procedural framework that incorporate procedures for IT security information, communication and reporting	There are informal *operational* IT security practices in SSU and ITS in areas of TRA, network monitoring and version/patch management. Also, there are IT security guidance/procedure gaps as set out in the Control Processes section. Under the RACI initiative, SSU and ITS are working on filling in these gaps with a priority on definition of IT security information, and the nature, scope and manner of IT security reporting including escalation of IT security matters to senior management. It is important that these improvements are incorporated into the IT security *procedural* framework. Interviews indicate that security policy and requirements and, in particular IT security, are not always well communicated to them. In addition, interviews with SafeNet smart card users indicated that their knowledge of security steps to follow, importance of securing the card when not in use, and potential exposure to OSFI should the card be misused varied widely.
Formalize and strengthen IT security policies and procedures into an overarching security program incorporating employee awareness training and training of Security and IM/IT staff.	In 2009 SSU conducted an all employee awareness program. SSU need to conduct *IT security awareness* training as part of an agency security plan for all employees to include an orientation to overall IT security in OSFI, and sessions on their respective roles and responsibilities in managing IT security, using of SafeNet, and safe use of their Laptop, Blackberry, e-mail and networking. From a *technical* IT and IT security perspective there is a need for cross training such that IT security analysts are comfortable with ITIL and IT analysts are comfortable with IT security risk and related MITS security requirements. It essential that SSU and IM/IT staff talk the same language. *We recommend strengthening the IT security procedural framework that incorporates procedures for IT security information, communication and reporting.* *We recommend formalizing and strengthening IT security policies and procedures into an overarching security program incorporating employee awareness training and training of Security and IM/IT staff.*

Conclusion

Overview

Our audit covered the *IT Security Access internal control* framework *as at December 2009* and improvements implemented and underway in the 3rd Quarter 2009-10 and forward, and a review of the application the SafeNet smart card security measure (restricted access to OSFI IT information) for the period *from April 2009 to the end of September 2009.*

The audit work was conducted on a collaborative basis involving information gathering and assessments, interviews with Security Services Unit and Infrastructure Technology Services, IM/IT, management and staff, and the use of SafeNet across the Office. We found that OSFI has a robust IT security architecture, *Diagram 1 - IT Security Architecture*. We also observed a commitment to establishing a comprehensive IT security access *internal control framework* on a consolidated collaborative basis

Conclusion

Our audit conclusion based on our assessment of the *IT Security Access internal control* framework is that:

> *Many components of the internal control framework are in place. There are key areas where improvements are required. The Office has undertaken initiatives and steps in establishing a comprehensive IT security access internal control framework. We recognize the effort undertaken in this regard.*
>
> *In order to address the areas requiring improvements, the participation of managers and management across the Office is needed as improvements affect all the Sectors and Divisions.*
>
> A focused effort is required in:
>
> - Formalizing and strengthening IT security policies and procedures into an overarching IT security program
> - Establishing a security risk management process at an operational level consistent with ERM practices
> - Strengthening the IT security procedural framework between Services Security Unit, and Infrastructure Technology Services & other IM/IT groups

Our audit team wishes to recognize the excellent exchange of views and support received throughout this audit.

_____ _____

Senior Director, Audit & Consulting Services

Date

Management Response

Both SSU and ITS view the audit as a positive contribution to our mandates. We thank the audit team for both their collaborative approach and depth of review. We are in full agreement with the findings. They reflect an unbiased indication of the progress we have made so far and paint an accurate picture what is left to accomplish. While there are solid core IT Security components in place, management recognizes that improvements in the IT Security Access internal control framework are necessary.

As set out in the report, OSFI has a comprehensive IT security architecture, as indicated in *Diagram 1- IT Security Architecture,* providing restricted access to OSFI's electronic information through security measures such as two factor authentication (i.e. *SafeNet* Smart Card), and communications, full laptop and PC data encryption. Independent threat and risk assessments, ongoing monitoring of OSFI's IT environment and daily vulnerability and risk assessments confirm that this is the case. Management is of the view that in light of the foregoing and the fact that, to date, no unauthorized access to OSFI electronic information has been brought to our attention, OSFI has a good IT security foundation in place.

We also note that the report recommendations highlight challenges ahead in further strengthening OSFI's IT Security Access internal control framework. A number of initiatives have already been undertaken to address these challenges and others are now underway such as establishing a working group to further developing the RACI matrix and building on the existing elements of the internal control framework

We are committed to a balanced approach of strengthening the security program at OSFI within an acceptable level of risk, so that it can be held up as a model of efficiency and effectiveness to other federal organizations. All recommendations are to be addressed during the 14 months from now through to the end of the 2010-2011 fiscal year.

Appendix A - Internal Control Criteria

Internal Control Criteria (used for audit evaluation purposes)	
Elements	**Components**
Governance: Objective setting & operating environment	▪ OSFI security governance, objectives, oversight accountabilities, and organization structures exist ▪ Roles and responsibilities consistent with the underlining competencies, and the interactions of stakeholders (senior management, ERM, sectors/divisions, audit and review, and those that provide and support security) are defined, communicated and understood ▪ OSFI's security policies and practices incorporate policy on government security (PGS) and management of information technology security (MITS) standards as adapted to OSFI's environment ▪ Security policy and guidance is in place that provides for restricted access to and protection of electronic information (defined, documented & communicated) and that is reviewed and changed as appropriate consistent with PGS requirements and MITS security standards ▪ Security policy and guidance regarding electronic information are aligned and supports the implementation of corporate 'plans and priorities'
Risk management	▪ External and internal risks related to security access to and protection of electronic information are identified, assessed, mitigation taken and incorporated into security policy, guidance ▪ The determination of security and IT requirements, and selection, testing and implementation of security measures/tools is based on the identification and assessment of risk ▪ External and internal IT environments are continuously monitored and assessed for threats and vulnerabilities, and incorporated into security risk management ▪ OSFI risk management and risk tolerance guidance is incorporated into security risk management
Control Processes	▪ Office-wide security *planning and resources* incorporate the requirements for providing security access to and protection of electronic information
	▪ There is a *security protection program* that includes monitoring of and supporting for security measures/tools such as smartcard, firewall, encryption, application security, and virus and malicious code protection, self-assessments and independent security audits/checks, access control and physical security measures
	▪ There is *incident management* for detecting and managing IT security incidents that access, modify, disrupt or circumvent security measures
	▪ Security requirements are incorporated into *system development* and over the life cycle of the application/system or service
	▪ *Continuity/ Recovery planning* and plans incorporate the requirements for providing security access to and protection of electronic information

Governance: Information, communications & reporting	▪ Security information related to access to and protection of electronic information is defined, gathered, assessed and incorporated into management, security and operations reporting ▪ Security information on monitoring, risk/vulnerability assessments, incident management and mitigation actions is communicated among security and stakeholders on a continuous basis consistent with respective governance and oversight accountabilities ▪ Security awareness and training of employees and those involved in security is defined, established and communicated