[*] An asterisk appears where sensitive information has been removed in accordance with the *Access to Information Act* and *Privacy Act*.

PRIVY COUNCIL OFFICE

Audit of Information Technology (IT) Security

Audit and Evaluation Division

Final Report

November 16, 2009

Table of Contents

Executive Summary

Audit Objective

The objective of this internal audit was to assess the adequacy of information technology (IT) security in order to safeguard the Privy Council Office's (PCO's) information assets.

Scope

The audit scope involved an assessment of the IT security function at PCO, including its governance and policy framework; management and business procedures dealing with risk and vulnerability management; processes for handling incidents, business continuity, systems development, security assessments, operational controls over network access and protection, and physical security; and resources and overall staff awareness.

The audit scope did not include the conduct of technical evaluations of controls such as the monitoring of network traffic, the attempted penetration of network protection, or the validation of firewall settings. [*]

Audit Conclusion

Recent years have seen rapid advances in information technology which have facilitated greater levels of interconnectedness in support of improved service delivery. At the same time there have been similar increases in the number and potential severity of threats to information and IT security. Within this dynamic environment, PCO has an evolving IT security infrastructure that is currently safeguarding the department's information assets. However, audit results have identified several areas where action is required by management to improve role clarity, security planning, security procedures and resource prioritization in order for PCO to continue to effectively safeguard its information assets.

Statement of Assurance

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 conclusion is based on a comparison of the conditions, as they existed at the time, against pre-established audit criteria that were agreed with management. The conclusion is applicable only to the entity examined. The evidence was gathered in compliance with Treasury Board policy, directives, and standards on internal audit.

Summary of Findings and Recommendations

[*]

Related to the overall IT security regime, the audit found areas where improvements are needed with respect to Business Continuity Planning (BCP). A Business Continuity Management (BCM) framework has been developed at PCO and is moving towards implementation. [*] At the departmental level, the need to strengthen business continuity planning has been identified in the Corporate Risk Profile and in a business case brought forward by Security Operations Division.

A challenging yet collaborative IT environment at PCO points to the achievability of medium-term improvements in IT security that would enhance existing relationships among all security stakeholders. The current management framework for IT security is highly dependent on [*] A sustainable IT security program involving all key stakeholders should be implemented to better assure management that priorities are being addressed. Furthermore the audit found that capturing procedures and processes in a documented form is an attainable and desirable objective for the longer-term transfer of IT security knowledge.

Our detailed recommendations are included in the body of this report. Management has indicated their agreement with all recommendations and has prepared a plan to implement corrective actions. The action plan prepared by management is presented in Section 3.0 of this report.

(Original signed by the Chief Audit Executive)

SIGNATURE OF CHIEF AUDIT EXECUTIVE
JIM HAMER

1.0 Introduction

1.1 Background

The Audit of Information Technology (IT) Security was approved as part of the Multi-Year Internal Audit Plan for the Privy Council Office (PCO) 2008-2009 to 2010-2011.

The current audit was led by the PCO Audit and Evaluation Division and contracted through Hallux Consulting Inc. An initial planning phase was undertaken during February and March 2009, the audit examination was done in April and May 2009. This audit follows on work conducted by auditors from Finance Canada who were working under a shared services agreement to provide internal audit services to PCO prior to the establishment of PCO's Audit and Evaluation Division. In May 2007, Finance Canada tabled a Preliminary Survey Report with the PCO Audit and Evaluation Committee. [*]

The PCO is governed by federal government policies, such as the *Government Security Policy* (GSP)[1]. The GSP defines the basic requirements to safeguard employees and assets, and to assure the continued delivery of services. In 2005, the Treasury Board Secretariat (TBS) requested that all departments – including PCO - implement by December 2006 the 144 standards from the *Management of Information Technology Security (MITS) Operational Security Standard*. MITS standards form the baseline requirements for departmental IT security programs so that federal departments, like PCO, can ensure the security of information and IT assets under their control. It also provides direction as to how departmental IT security programs should be organized; identifies roles, responsibilities and accountabilities for IT security; and identifies technical and operational safeguards in line with the GSP that focus on prevention, detection, response, and recovery safeguards.

TBS requires departments and agencies to carry out periodic internal audits to assess their compliance with the GSP and the effectiveness of its implementation.

1.2 Objective

The objective of this internal audit was to assess the adequacy of IT security in order to safeguard PCO's information assets.

[1] On July 1, 2009 the Treasury Board *Policy on Government Security* replaced the *Government Security Policy*.

1.3 Scope

The audit scope involved an assessment of the IT security function at PCO, including its governance and policy framework; management and business procedures dealing with risk and vulnerability management; processes for handling incidents, business continuity, systems development, security assessments, operational controls over network access and protection, and physical security; and resources and overall staff awareness.

The audit scope did not include the conduct of technical evaluations of controls such as the monitoring of network traffic, the attempted penetration of network protection, or the validation of firewall settings. [*]

1.4 Approach and Methodology

The audit followed a generic approach to MITS compliance developed by the audit team. MITS components were aligned with four TBS Management Accountability Framework (MAF) components, those being Accountability, Risk Management, Stewardship, and People. Audit criteria are presented in Appendix A.

2.0 Audit Findings, Conclusions and Recommendations

For the purposes of this internal audit, the report is formed around three main themes of findings surrounding IT Security at PCO: 1) Immediate Security Improvements, 2) IT Security Program and 3) Formal IT Security Procedures. Since IT security encompasses many elements, the audit produced several findings, some positive and some requiring management attention. The following sections detail the audit team's resultant findings, conclusions and recommendations.

2.1 Immediate Security Improvements

Related to the overall IT security regime, the audit found areas where improvements were necessary and reasonable in the short-term. The audit expected to see: a standard program of best practices in use around physical and media protection; an effective, well documented, well-operated program of network security and protection; and, a Business Continuity Management (BCM) framework that included a governance structure, a fully documented, up-to-date and tested IT Business Continuity Plan (BCP) and Information Technology Disaster Recovery Plan (ITDRP).

Physical Security and IT Media

[*] The audit found [*]. In addition security personnel are positioned at strategic entrances. Procedures and processes that are in place to secure, mark, transport and retire backup media are in line with MITS and best practices.

[*] however, access to the server room is appropriately controlled. Within the server room, equipment is appropriately labeled [*]. The Informatics and Technical Services Division (ITSD) of the Corporate Services Branch (CSB) is currently involved in rationalizing their equipment in the effort to improve efficiency and reduce costs. [*]

Network Security

While physical security is a key security feature and represents the first line of defence for the IT security environment, network safeguards are a combination of hardware components, software tools and necessary functions carried out by expert staff. [*]

Business Continuity

The protection of the IT network through physical security and network safeguards helps to ensure that IT services can be delivered on an on-going basis. Furthermore, [*]. A valid (i.e. up-to-date and tested) ITDRP is a key management tool to mitigate the risk of outright IT systems failure and comprises an essential element of an organization's business continuity strategy.

[*]

Conclusion

[*]

Recommendation

1. ***The Assistant Deputy Minister, Corporate Services Branch:***
   [*]

2.2 IT Security Program

A challenging yet collaborative IT environment at PCO points to the achievability of medium-term improvements in IT security. The audit expected to see a comprehensive IT Security Program led by an experienced and qualified IT Security professional as the IT Security Coordinator (ITSC). The audit also looked for evidence that the intent and direction of GSP/MITS was evident in key roles, including the Departmental Security Officer (DSO), the Chief Information Officer (CIO), the BCP Coordinator and the ITSC, as well as in the security management structure.

Governance

The audit found that a good working relationship exists among key players in security, a fact acknowledged by all participants. An appropriate discussion about roles and responsibilities for security is underway within PCO [*]. The role of ITSC is assigned to the Chief IT Security, who reports to the Executive Director ITSD, CSB. The incumbent ITSC has [*] to facilitate an effective IT security program at PCO. [*]

The management of IT security requires collaboration between the DSO, the ITSC and the CIO. The Executive Director of ITSD assumes the role of CIO as referenced in the position description of the Executive Director, although the CIO role is not formally described in PCO Security Policy. The Corporate Information Services Division (CISD) of CSB provides leadership for information management (IM) for PCO. [*]

ITSD has made progress in documenting IT project management requirements, and, as a consequence, IT security implications. For example, IT project management controls have been improved through the recent creation of the Business Solutions Management Group (BSMG) within ITSD and subsequent development of project management and delivery documentation. [*] The audit acknowledges that the [*] at present. [*]

Policy

Every federal department must have a departmental IT security policy to meet GSP and MITS requirements. PCO has a security policy [*] that is a mixture of policy, procedures and guidelines. [*]

Security Program Planning

The ongoing funding for security is established within the annual budgetary cycle at PCO and consequently addressed for IT security at the operational level, including funding for IT security requirements in major projects. Furthermore, [*]

Managers and staff in PCO are generally aware of information sensitivity and day-to-day conventions for minimizing the risk to information security. A rule-based approach to security awareness is in place in the department [*]. Training should continue to be made available to PCO employees to help them maintain a high understanding of the requirements of security policies and to help them understand how to work within existing security protocols. [*]

Conclusion

[*]

Recommendation

2. ***The Assistant Deputy Minister, Corporate Services Branch in collaboration with the Deputy Secretary to the Cabinet, Foreign and Defence Policy,*** [*]

3. ***The Deputy Secretary to the Cabinet, Foreign and Defence Policy, continue to make available security training to PCO employees to help them maintain a high understanding of the requirements of security policies and to help them understand how to work within existing security protocols .***

2.3 Formal IT Security Procedures

Capturing procedures and processes in a documented form is an attainable and desirable objective for the longer-term transfer of IT knowledge. The audit expected to see a formal set of related IT and IT Security procedures consistent with MITS expectations, including: a formal risk management and vulnerability assessment program; a formal process for incident management; a standard set of best practices for use in the system development life cycle with associated management and techniques; a program of audit and assessment of IT security and a standard and functioning access management process; and, best practices in the management of cryptographic keys and equipment.

Risk Management

Risk management is performed as one of the functions associated with project management and budget review. The IT operational budget provision is analyzed, as part of the projects and security initiatives cycle, annually (as a minimum) or on an as required basis. A set of risk management practices exist: [*] on an annual or bi-annual basis. PCO IT and security personnel are aware of security issues associated with the uniqueness of the PCO environment, nevertheless [*]

Incident Management

Incidents are managed on an [*]

Certification and Accreditation

The IT security process is an integral part of a system development life cycle to certify and accredit software for operation on PCO networks. ITSD documentation identifies their role in the support and maintenance of software packages. [*]

Access and Encryption

The nature of access control and encryption make them vital elements associated with confidentiality and integrity of the IT environment. Both elements must perform at expected levels in order for protection to be assured. [*] accounts no longer required are deleted or de-activated based on change requests. Encryption and related activities [*]

Audit and Assessment

Self-assessments are performed as per MITS and are properly documented, [*]

Conclusion

[*]

Recommendation

4. ***The Assistant Deputy Minister, Corporate Services Branch ensure*** [*]

3.0 Management Response and Action Plan

Audit of IT Security

The Assistant Deputy Minister, Corporate Services Branch and the Deputy Secretary to the Cabinet, Foreign and Defence Policy have overall accountability for the Action Plan.

Recommendation	Actions to be Taken	Responsibility	Target Date
1. ***The Assistant Deputy Minister, Corporate Services Branch:*** [*]	Management agrees with the recommendation. [*]	Assistant Deputy Minister, Corporate Services Branch	Nov 2009
[*]	Management agrees with the recommendation. [*]	CIO	January 2011
2. ***The Assistant Deputy Minister, Corporate Services Branch in collaboration with the Deputy Secretary to the Cabinet, Foreign and Defense Policy,*** [*]	Management agrees with the recommendation. Management will ensure that: [*]	DSO CIO	a) May 2010 b) January 2010
[*]	Management agrees with the recommendation. [*]	DSO & CIO	Aug 2009
[*]	Management agrees with the recommendation. [*]	Assistant Secretary to Cabinet, Security and Intelligence	May 2010

Recommendation	Actions to be Taken	Responsibility	Target Date
[*]	Management agrees with the recommendation. [*]	DSO & CIO	Aug 2009
3. The Deputy Secretary to the Cabinet, Foreign and Defence Policy, continue to make available security training to PCO employees to help them maintain a high understanding of the requirements of security policies and to help them understand how to work within existing security protocols.	Management agrees with this recommendation. - Training and awareness sessions have been developed to assist employees in properly marking classified documents and in the proper transmission and destruction of classified documents.	DSO	On-going
4. The Assistant Deputy Minister, Corporate Services Branch ensure [*]	Management agrees with this recommendation. [*]	Deputy Director, IT Security	Mar 2010
[*]	Management agrees with this recommendation. [*]	Deputy Director, IT Security	Mar 2010
[*]	Management agrees with this recommendation. [*]	Deputy Director, IT Security & Deputy Director, Business Solutions Management	June 2011
[*]	[*]	Deputy Director, IT Security	June 2011

Appendix A: Audit Criteria

TBS Management Accountability Framework (MAF) Element	MITS Component
Accountability. Accountabilities for results are clearly assigned consistent with resources, and delegations are appropriate to capabilities. Key words: clear delegations, responsibilities, cascading commitments, Performance Management Agreement	**Organization (Governance).** A well-defined security organization outlines the roles, responsibilities, and interaction of senior management, risk managers, program owners, security experts, and employees for IT security. An effective IT security program delegates IT security functions among these roles, inculcates a common understanding of security responsibilities, and promotes a high degree of interaction.
	Policy. Every department must have a departmental IT security policy to apply GSP and MITS requirements within the departmental context and to establish fundamental departmental commitments.
Risk Management. The executive team clearly defines the corporate context and practices for managing organizational and strategic risks proactively. Key words: key risks identified, part of decision making culture.	**Risk Management.** Risk management is fundamental to an effective IT security program. IT security experts must manage risk continuously, as threats and operational environments are constantly changing. Senior management, risk managers, program owners, and security experts must be engaged in managing and incorporating IT security risks into the overall corporate risk profile. A strong risk management program takes into account threats, vulnerabilities, impacts, probabilities, and safeguards.
	Vulnerability Management. Vulnerabilities can emerge at any stage in the development or operation of an IT system. Vulnerability management underlies risk management. Once vulnerabilities are discovered, the corresponding risk must be either mitigated or accepted.
	ID of IT Assets. Identification of critical IT assets is essential to establishing business priorities to protect the critical and most important services and to mitigating security risks in order of their magnitude.
Stewardship. The departmental control regime (assets, money, people, etc) is integrated and effective, and its underlying principles are clear to all staff. Key words: systems provide relevant info, audit function, compliance with policy, regulations, legislation.	**Incident Management.** IT security incidents that access, modify, disrupt, or circumvent a system could have a significant impact on the delivery of programs and services. Like vulnerability management, departments must be vigilant in looking for, detecting, and managing incidents.

TBS Management Accountability Framework (MAF) Element	MITS Component
Stewardship (continued)	**Continuity Planning.** Continuity planning ensures the availability of assets necessary to maintain government operations. Information management (IM) and IT continuity planning are integral elements of business continuity planning (BCP).
	System Development Life Cycle (SDLC). It is easier, more cost efficient, and more secure to implement IT security safeguards during the design and implementation of a program or service rather than after it is established.
	Assessment and Audit. Annual security review programs are essential for senior managers who require an overview of problem areas that affect departmental business lines to have the information they need to take appropriate action. Review programs will consist of appropriate performance measurement tools, including self-assessment tools, and independent audits.
	Operational Controls. – Physical Security and IT Media – Access Control and Encryption – Network Safeguards
People. The department has the people, work environment and focus on building capacity and leadership to assure its success and a confident future for the Public Service of Canada. Key words: renewed sustained capacity, supportive workplace, leadership.	**Resources.** New and expanding programs and services must allocate adequate resources to ensure IT security requirements are met. IT security resources should be identified in the business planning process; insufficient availability of adequate human resources and funding is among the biggest risks facing MITS implementation.
	Awareness. Departments must regularly inform all personnel of their IT security roles and responsibilities. Awareness is an essential requirement to improve understanding of IT security risks and to close the gap between business owners and the IT security community.

Appendix B: List of Acronyms Used

Business Continuity Management	BCM
Business Continuity Plan	BCP
Business Solutions Management Group	BSMG
Chief Information Officer	CIO
Corporate Information Services Division	CISD
Communications Security	COMSEC
Communications Security Establishment	CSE
Departmental Security Officer	DSO
Government Security Policy	GSP
Informatics and Technical Services Division	ITSD
Information Management	IM
Information Technology Disaster Recovery Plan	ITDRP
Information Technology Security Coordinator	ITSC
Management Accountability Framework	MAF
Management of Information Technology Security	MITS
Risk Management	RM
Threat and Risk Assessment	TRA
Vulnerability Assessment	VA