National Defence Défense nationale

Assistant Deputy Minister (Review Services)

Reviewed by ADM(RS) in accordance with the *Access to Information Act*. Information UNCLASSIFIED.

Security Audits: Management Action Plan Follow-up

December 2015

1850-3-003 (ADM(RS))

Canada

Caveat

The result of this work does not constitute an audit of the security control areas. Rather, this report was prepared to provide reasonable assurance that Management Action Plan (MAP) items resulting from the various security audits were implemented as stated and as such have addressed the associated recommendations.

Table of Contents

Acronyms and Abbreviations

ADM(RS)	Assistant Deputy Minister (Review Services)
BCP	Business Continuity Planning
CAF	Canadian Armed Forces
CDS	Chief of the Defence Staff
DGDS	Director General Defence Security
DM	Deputy Minister
DND	Department of National Defence
DSO	Departmental Security Officer
DSP	Departmental Security Plan
DSX	Defence Strategic Executive Committee
FY	Fiscal Year
IM	Information Management
IT	Information Technology
L1	Level 1
MAP	Management Action Plan
NDSOD	National Defence Security Orders and Directives
SRT	Security Reform Team
TBS	Treasury Board Secretariat
VCDS	Vice Chief of the Defence Staff

Introduction

In keeping with the Treasury Board Policy on Internal Audit,[1] Assistant Deputy Minister (Review Services) (ADM(RS)) is required to undertake audit follow-ups to assess the implementation status of Management Action Plan (MAP) items developed in response to previous ADM(RS) audit recommendations. In accordance with the Chief Review Services[2] Risk-Based Audit Plan for fiscal year (FY) 2015/16 to 2017/18, this audit follow-up was selected to determine MAP progress for the following audits:

- Audit of Security of Sensitive Inventories (May 2004)
- Audit of Security Clearance Process (September 2006)
- Audit of Security Incident Management (June 2010)
- Audit of Industrial Security (May 2011)
- Audit of Sanitization and Destruction of Information Management (IM)/Information Technology (IT) Assets (December 2012)
- Audit of Business Continuity Planning (BCP) (October 2013)

Two other security related audits conducted during the same timeframe were not included in this follow-up. The Audit of IT Security: Certification and Accreditation Process was not selected because the certification and accreditation process has been replaced with the Security Assessment and Authorization process. An audit of this new process is planned for FY 2017/18. Additionally, the security posture assessments conducted on the Defence Wide Area Network and the Consolidated Secret Network Infrastructure, with the assistance of the [redacted]

Methodology

This audit follow-up is based on a review of documentation and evidence to assess the progress made in implementing the MAP items. The following methods were used to assess progress:

- detailed assessment of the progress of the MAP items reported by the office of primary interest;
- interviews with key stakeholders; and
- examination of supporting documentation.

This follow-up does not represent a second audit of the same issues. Instead, it is an assessment of the progress made towards implementing the MAP items. No testing was performed to determine whether the action plans were achieving the desired results.

[1] Treasury Board Policy on Internal Audit. http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/ia-vi/ia-vi_e.asp
[2] Chief Review Services is the former designation of ADM(RS). The ADM(RS) designation came into effect on May 15, 2015.

Statement of Conformance

The audit follow-up conclusions contained in this report are based on sufficient and appropriate audit evidence gathered in accordance with procedures that meet the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*. The audit follow-up thus conforms to the Internal Auditing Standards for the Government of Canada, as supported by the results of the quality assurance and improvement program. The opinions expressed in this report are based on conditions as they existed at the time of the audit follow-up and apply only to the entity examined.

Context

ADM(RS) has conducted a number of security-related internal audits since 2004. It has also completed various follow-up audits in this timeframe to determine progress made toward implementing the specific MAP items. Efforts have been made over the past decade to address shortcomings. However, until now, little progress has been made in part because the Departmental Security Officer (DSO) had neither the authority over the affected security process nor the personnel to implement the required changes. More significantly, having an outdated departmental security policy made it impractical to amend or improve processes without first addressing the policy issue.

In order to address the identified issues, the Deputy Minister (DM) and the Chief of the Defence Staff (CDS) issued an initiating directive in March 2013 to the Vice Chief of the Defence Staff (VCDS) to establish a Security Reform Team (SRT). The team’s objective was to conduct a full review of the existing security program, recommend ways to address previously identified shortcomings, and provide recommendations for the development of a more robust Defence Security Program. The SRT review was conducted over an eight-month period beginning in March 2013, and the findings and recommendations were presented to the Defence Strategic Executive Committee (DSX) in November 2013.

The SRT findings were consistent with those identified in the ADM(RS) audits conducted between 2004 and 2013. Key SRT program findings included the following:

- [redacted]
- [redacted]
- [redacted]
- [redacted]

The SRT provided the DSX with numerous program and process recommendations designed to address the more significant program issues. Some of the key program recommendations included the following:

- centralization of the security organization, whereby the organization would exercise a more robust functional authority, retain current line authorities, and assume responsibility for personnel security, industrial security, physical security, and identity management;
- upgrading the rank of the DSO to ensure appropriate visibility given the complexity of the security program; and
- development of a comprehensive security policy that would include clearly defined security authorities.

The DSX supported all of the recommendations, including the implementation of a revamped Defence Security Program that would provide the DSO with "full functional authority over the program and command authorities over selected processes."[3] In addition, the DM and CDS assigned the DSO additional responsibilities for oversight of the security threat and risk assessment and information assurance.

To further strengthen this authority, in March 2014, the VCDS established the Director General Defence Security (DGDS) organization. The DM/CDS then appointed the director general as the DSO and upgraded the rank from colonel to brigadier general. The DGDS/DSO was made responsible for defence security including leadership, development, and management of the entire Defence Security Program and was made accountable to the DM/CDS for the effective, efficient, and integrated management of the program.[4]

To fulfill this responsibility, four directorates were created within DGDS, and considerable time and effort was expended staffing the organization. The DSX also approved the creation of six regional DSO positions with the role of providing functional security support and coordination to the DSO to manage and implement the security requirements.

As part of the restructuring of the security program and to strengthen the overall governance structure, the Senior Security Advisory Committee was re-established and held its first meeting in December 2014. The committee is chaired by the VCDS, and it provides guidance and oversight of the Defence Security Program so as to ensure that the program is managed in an effective, efficient, and integrated manner. The committee also ensures security activities, requirements, and the impact of changes in government and departmental policies are known and understood by the Department of National Defence and Canadian Armed Forces (DND/CAF) organizations responsible for the implementation of appropriate force protection and security measures.[5] The establishment of this senior body is another component of the security program that sets the foundation to improve and strengthen security program governance.

[3] DG SRT. VCDS Defence Security Renewal Action Directive, November 26, 2013.

[4] National Defence Security Orders and Directives (NDSOD), Chapter 1 – National Defence Security Program and Responsibilities.

[5] Senior Security Advisory Committee Terms of Reference (Approved October 2014).

Progress towards MAP Implementation

The objective of the audit follow-up was to assess progress made towards implementation of the MAP items. However, doing so would not accurately reflect the level of effort expended by the DGDS organization in developing the foundation required to ensure that any process changes would be implementable, resolve the identified shortcomings, and comply with established policy.

Significant progress has been made in establishing the foundation required to develop and implement a strong Defence Security Program. In particular, establishing and staffing the DGDS organization, completing the Departmental Security Plan (DSP), and publishing a security policy suite that supersedes all existing directives (National Defence Security Policy, National Defence Security Instructions, and National Defence Security Manual) comprise the basis and means for addressing the outstanding MAP items.

That being said, a summary of the audit findings from the original audits and an indication of any progress specific to the audit findings can be found in Annex A.

DSP

A key priority for the DSO over the last year has been to complete the DSP. The Policy on Government Security states that "Deputy heads of all departments are responsible for approving the DSP that details decisions for managing security risks and outlines strategies, goals, objectives, priorities and timelines for improving departmental security and supporting its implementation".[6] Since the DSO is functionally accountable to the deputy head, he/she is responsible for developing, implementing, monitoring, and maintaining the DSP.[7] While the TBS requirement was to have a DSP fully implemented by June 2012, DND was granted an extension to that requirement.

In May 2015, the DM and the CDS formally approved the DSP, and there is a commitment to review and update it annually.[8] The DSP identifies security risks for all the Treasury Board Secretariat (TBS) security control objectives, as well as for the three additional security control objectives specific to DND/CAF (force protection, identity management and travel security). The plan outlines security program objectives, priorities, and [redacted] for addressing identified departmental security risks.

Having been provided with formal authority, responsibility, the DSP, and resources, the DSO is now in a better position to implement the security process changes required to reduce security risks across the Department and ensure compliance with policy.

[6] TBS Policy on Government Security, 2009.
[7] TBS Directive on Departmental Security Management, 2009.
[8] DND/CAF DSP, May 2015.

Policy and Direction

ADM(RS) reports have consistently noted that security policy documents were unclear and outdated. The VCDS issued a Renewal Action Directive[9] in November 2013 and stated that one of the main focuses for the near term had to be updating the policy suite. The VCDS indicated that the DM/CDS supported a full, comprehensive security policy suite renewal. The VCDS also noted that within the policy renewal, there needed to be an overarching policy document containing a defence security policy statement that would be signed by the DM and CDS.

After extensive effort and consultation with all the Level 1s (L1), the NDSOD were published in June 2015. Defence Administrative Order and Directive 2006-0 – Defence Security designates DGDS as the DSO and recognizes the establishment of the NDSOD. The NDSOD clarify roles, responsibilities, and authorities for DGDS, L1s, and all DND/CAF personnel as it relates to security. The NDSOD have 16 chapters, covering all TBS security control objectives and the three security control objectives specific to DND. Therefore, DGDS can now begin to focus on developing plans to implement the requirements of these new directives and on improving current process rigour.

Training

In an effort to address the ADM(RS) and SRT finding regarding the lack of security training and awareness across the Department and to ensure compliance with the TBS policy, DGDS developed a mandatory online security awareness training course for all DND/CAF personnel. This was strengthened by the release of a Canadian Forces General Order in December 2014 indicating the requirement to complete the course. Personnel in the National Capital Region were required to complete the course by March 31, 2015, and all other employees and CAF members were required to complete the course by June 30, 2015. As of April 1, 2015, 65% of personnel in the National Capital Region had completed the online course.[10] This department-wide, high-level training is a good start in addressing the issues with respect to the lack of training and awareness.

Risk Treatment Plans

The development of the DSP helped DGDS identify and assess departmental security risks. DGDS consulted each of the L1s in order to identify security risks relevant to their organization. It assessed these risks and subsequently developed “risk treatment plan objective statements” for each of the identified risks. These objectives are found in DGDS’s security risk register and will be used to develop mitigation plans for the identified security risks.

The audit team reviewed the risk treatment plan/security risk register to ensure that the findings from the ADM(RS) security audits had been reflected in the plans. While some of these findings have already been addressed | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

[9] VCDS. Defence Security Renewal Action Directive. November 24, 2013.
[10] Senior Security Advisory Committee, Meeting Record and Decision Sheet, April 1, 2015.

[redacted]

DGDS is currently expecting a progress update for year one commitments made in the DSP by October 2015. Detailed work plans including scope requirements, business planning, and sequencing of tasks have started for commitments in years two and three of the DSP. These plans should articulate the steps to develop and implement the process changes required to address the security process rigour issues identified in previous ADM(RS) audit reports, and they should ensure compliance with the new departmental security policy suite. Upon completion of these detailed plans, the Department will then be in a better position to monitor progress towards completion of each MAP and ensure identified risks are being properly mitigated.

Conclusion

Significant progress has been made toward establishing the governance structure for defence security and setting the foundation to improve the effectiveness of the security program. Focus now needs to shift to maturing the governance structure and strengthening the processes and controls in order to reduce identified security risks across the Department and ensure compliance to policy.

Until all MAP items are fully implemented, current departmental security processes intended to protect personnel and ensure information, assets, and services are safeguarded from compromise [redacted] That being said, a strong foundation is now in place to facilitate the implementation of the changes required to strengthen the Defence Security Program.

Annex A—MAP Progress

Audit of Security for Sensitive Inventories (2004)

Original Audit Assessment

The Department [redacted]

Original Audit Findings

- The Department does not know [redacted]
- Physical security policy is too prescriptive and implementation of risk mitigation options is not linked to risk assessment results.
- [redacted]
- Local management has a responsibility [redacted]

Progress to Date

- NDSOD Chapter 15 has been released, providing a definition and examples [redacted]
- DGDS is developing an implementation plan to address DSP risk treatment plan objectives.
- DGDS is currently working on an implementation plan for the conduct of threat risk assessments that will build on lessons learned from reviewing physical security surveys and threat risk assessments received from some Defence sites.

Audit of the Security Clearance Process (2006)

Original Audit Assessment

The Department’s personnel security clearance process [redacted]

Original Audit Findings

- [redacted]
    - [redacted]
    - [redacted]
- [redacted]
    - [redacted]
    - [redacted]
- [redacted]
    - [redacted]

Progress to Date

- A draft business plan with goals and requirements [redacted] has been developed. Detailed plans, as they relate to specific MAP items, are still required.
- There is a plan to conduct a [redacted] to assist in developing options to address process shortcomings noted in the 2006 audit.
- Identity management and the security clearance groups within DGDS have been amalgamated.
- The new departmental policy requires that Director Personnel Security Identity Management, not the line manager, grant reliability status.
- A business case analysis of [redacted] is being conducted.

Audit of Security Incident Management (2010)

Original Audit Assessment

The Department [redacted]

Original Audit Findings

- [redacted]
- [redacted]
- There is insufficient evidence to confirm that [redacted]
- There is insufficient evidence to confirm that [redacted]
- [redacted]

Progress to Date

- DGDS is in the process of developing a plan to address risk treatment plan objectives.
- DGDS is currently working on harmonizing the security incident management process.
- DGDS plans to [redacted]
- DGDS has developed a new policy that requires organizations to maintain a Unit Security Incident Register of all incidents originating within their unit and to report this information to DGDS on a semi-annual basis.
- DGDS is developing a process to maintain strategic oversight of [redacted]

Audit of Industrial Security (2011)

Original Audit Assessment

The Department's industrial security practices [redacted]

Original Audit Findings

- The Provost Marshal [redacted]
- Mandate and objectives of the industrial security program are not well established.
- [redacted]
- [redacted]
- [redacted] throughout the life of a contract.
- Office of the Auditor General audits:
  - 2007: This audit determined that [redacted]
  - 2013: This audit determined that [redacted]

Progress to Date

- NDSOD Chapter 8 states that a Security Requirement Check List must be completed for all contracts whether there are security requirements or not.
- A new Security Identification Document is needed for all contracts with security requirements. This will replace the Project Identification Document. These documents are essentially the same; however, the security identification document is required for all contracts rather than just for projects.
- DGDS staff have started to provide specific contract security training to units.
- Public Works and Government Services Canada will no longer process a DND contract unless the contract is accompanied by a Security Requirement Check List.

Audit of Sanitization and Destruction of IM/IT Assets (2012)

Original Audit Assessment

Current processes related to the governance and risk management of the sanitization and destruction of IM/IT assets [redacted]

Original Audit Findings

- [redacted]
  - [redacted]
  - [redacted]
- [redacted]
- [redacted]

Progress to Date

- DGDS has developed [redacted]
- Publication of NDSODs:
  - Chapter 6 – Security of Information highlights the requirement to ensure information is disposed of correctly; however, specific procedures for destroying information are still under development. Reference is made to various Government of Canada policies.
  - Chapter 7 – Information Security is a section on data storage media protection and provides more direction on the destruction of IT assets. It makes reference to Information Technology Security Guidance 06, clearing and declassifying electronic data storage devices.
- Sanitization control requirements are addressed in the DND/CAF IT Security Control Catalogue. The implementation and maintenance of these controls for specific IT systems and networks should be confirmed and validated through the Security Assessment and Authorization process.
- The DND/CAF IT Security Standard on portable/mobile data storage devices has been drafted and is expected to be promulgated by the end of December 2015. It will address the TBS Information Technology Policy Implementation Notice 2014-01, which details the new requirements for clearing and disposal of information from portable/mobile data storage devices.

Audit of Business Continuity Planning (2013)

Original Audit Assessment

A BCP governance structure with clearly defined roles and responsibilities was established in 2007. [redacted]

Original Audit Findings

- [redacted]
- [redacted]

Progress to Date

- Accountabilities, responsibilities, and authorities have been defined as part of NDSOD Chapter 10 on BCP.
- Focus is on developing the National Capital Region Level 0 and L1 interim BCPs.
- Initial consultations have taken place with L1 BCP coordinators, who have provided clarification on their initial input to the interim National Capital Region BCP.
  - Process to identify critical assets and services has begun.
  - An Intradepartmental Committee on BCP has been established.
- A methodology and a template, to be added to the policy suite, is being developed to assist L1s in the writing of both business impact and threat risk assessments.