National Defence | Défense nationale

ASSISTANT DEPUTY MINISTER (REVIEW SERVICES)

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

Audit of Information Technology Security: Roadmap Implementation



May 2016

7050-33-10 (ADM(RS))

Canada

Table of Contents

Acronyms and Abbreviations

ADM(IM)	Assistant Deputy Minister (Information Management)
ADM(RS)	Assistant Deputy Minister (Review Services)
CDS	Chief of the Defence Staff
DGDS	Director General Defence Security
DIM Secur	Director Information Management Security
DM	Deputy Minister
DND/CAF	Department of National Defence and the Canadian Armed Forces
DSO	Departmental Security Officer
DSP	Departmental Security Plan
IM	Information Management
IMB	Information Management Board
IT	Information Technology
ITSC	Information Technology Security Committee
OPI	Office of Primary Interest
SSAC	Senior Security Advisory Committee
VCDS	Vice Chief of the Defence Staff

Results in Brief

As a result of the Security Reform Team review in 2013, there has been significant evolution of the Department of National Defence and the Canadian Armed Forces (DND/CAF) Security Program and a renewed commitment by senior management to improve how the Program is governed and managed. For example, the Vice Chief of the Defence Staff (VCDS) established the Director General Defence Security (DGDS) organization, and the position was appointed as the Departmental Security Officer (DSO). At the same time, DGDS was delegated full functional authority for the Defence Security Program, and the Assistant Deputy Minister (Information Management) (ADM(IM)) retained the functional authority for Information Technology (IT) Security—one element of the Security Program.

Overall Assessment

- The IT Security governance structure needs to further evolve to provide authoritative direction and expectations, and effective coordination with the Defence Security Program.
- Processes to support management of and accountability for IT security plans need to be established.

ADM(IM) is supported by the IT Security Coordinator, Director Information Management Security (DIM Secur), who is also the delegated IT Security Authority in the Department. While a new Defence Security Program framework was established to support the DSO's functional authority, the Department has not conducted an equivalent review of the IT Security governance framework, and as such, the IT Security Program has not evolved in a similar fashion.

Under authority of a VCDS directive, DIM Secur was made responsible for developing the IT Security Roadmap that was to provide an overview of the IT Security Program. The desired end state was a department-wide, coordinated, and prioritized list of activities that would ensure IT Security priorities were addressed in the most efficient and timely manner with minimal duplication.

The 2014/15 to 2015/16 Risk-Based Audit Plan included an Audit of IT Security. The objective of the audit was to assess the governance and control practices in place to ensure implementation of the IT Security Roadmap. The audit found that there is an opportunity to strengthen the governance and control practices for the IT Security Program in order to support ADM(IM) in effectively exercising its functional authority for IT Security across the Department. Strengthening governance and control practices would also set the foundation for assigning accountability for achieving IT Security objectives, priorities, and expectations in the DND/CAF as set out in the IT Security Roadmap.

Findings and Recommendations

Finding. The IT Security Program needs to be supported by authoritative direction for program objectives and priorities based on a common understanding of risk, existing controls, and associated gaps. Authorities to establish and manage the IT Security Program are defined; however, the delegated authorities were not effectively exercised and supporting governance bodies and processes were not in place. Evolving the governance framework will support ADM(IM) in exercising the functional authority for IT Security and provide for better coordination with the Defence Security Program.

It is recommended that ADM(IM) do the following:

- develop the governance framework in support of exercising the functional authority for IT Security across the DND/CAF; and
- establish processes to define IT Security Program objectives and priorities within the context of the governance framework (to be developed) and identified risks.

Finding. The necessary processes to ensure that responsible organizations resource and execute IT Security plans were not established. DIM Secur has assigned staff to develop and implement processes to horizontally coordinate, monitor, and report on implementation of the IT Security Roadmap. Once established, these processes should provide the necessary information to hold responsible organizations accountable for their contribution towards achievement of objectives and their impact on residual risk. They should also provide valuable information that could be used to reassess risks and program level objectives and priorities.

It is recommended that ADM(IM) do the following:

- establish processes to horizontally coordinate, monitor, and report on the IT Security Program's objectives, priorities, and activities; and
- develop the accountability mechanisms, within the context of the governance framework for IT security (to be developed), to include progress, performance, and impact on residual risk at the corporate, program, and system levels.

Note: Please refer to Annex A—Management Action Plan for the management response to the Assistant Deputy Minister (Review Services) (ADM(RS)) recommendations.

1.0 Introduction

1.1 Background

In response to numerous audits highlighting the need for improvement throughout the Defence Security Program, the Deputy Minister (DM) and the Chief of the Defence Staff (CDS) established a Security Reform Team in March 2013. The Security Reform Team was tasked to conduct a full review of the Defence Security Program and provide recommendations to develop a more robust and capable Program and address risks identified in previous audits. Their recommendations were approved by the DM and CDS, resulting in significant changes to the Program. New management structures were established, policies were renewed, resources were allocated, and plans were developed to address identified risk areas.

The IT Security Roadmap was developed in March 2014, subsequent to approval of the Security Reform Team recommendations, to provide an overview of the IT Security Program—one element of the broader Defence Security Program. The desired effect was to provide a basis for ensuring that IT security priorities were addressed across the Department in the most efficient and timely manner.

The 2014/15 to 2015/16 Risk-Based Audit Plan included an Audit of IT Security. A renewed focus on effective management and execution of the Defence Security Program made it timely to look at the supporting governance and control mechanisms in place to ensure the IT Security Roadmap would be implemented to manage associated security risks.

1.1.1 Government of Canada Policy on Government Security

Government of Canada policy identifies requirements to ensure that deputy heads effectively manage security activities within departments and contribute to effective government-wide security management.

The DM and CDS, as the deputy heads for the DND/CAF, are responsible[1] for establishing a security program that includes the following:

- has a governance structure with clear accountabilities;
- has defined objectives that are aligned with departmental and government-wide policies, priorities, and plans; and
- is monitored, assessed, and reported on to measure management efforts, resources, and success toward achieving its expected results.

They are also responsible for appointing a DSO to manage the security program. This includes responsibilities for planning, establishing governance, managing security risks, monitoring and oversight, measuring and evaluating performance, and providing government-wide support. The DSO is required to be functionally responsible to the DM and CDS in fulfilling his/her responsibilities.

[1] Treasury Board Secretariat, Policy on Government Security, July 1, 2009.

For IT security, departments must appoint an IT security coordinator with at least a functional reporting relationship to both the departmental Chief Information Officer and the DSO.[2] The IT security coordinator responsibilities include establishing and managing a departmental IT security program as part of a coordinated departmental security program, providing advice, monitoring compliance, and serving as the Department's primary IT security contact.

Departments are responsible for selecting, implementing, monitoring, and maintaining sustainable security controls to achieve security control objectives.[3] The Treasury Board Secretariat Directive on Departmental Security Management identifies 15 areas for security control objectives, including IT security, to be achieved by departments. Departments can select and implement additional security controls based on the results of their risk assessments. A Departmental Security Plan (DSP) is required to detail security risk management decisions and outline the strategies, goals, objectives, priorities, and timelines for improvements.

1.1.2 Defence Security Program

With the approval of the Security Reform Team recommendations, the VCDS established the DGDS organization, and the DM and CDS delegated the DSO functional authority[4] for the entire Defence Security Program to this position. The organization's ability to deal with security issues has since evolved rapidly along a maturity continuum. Despite the fact that some security program elements (e.g., personnel security, physical security) were centralized under DGDS, functional authorities for other security program elements, including IT Security, remained outside the purview of the DGDS organization. In order for the DSO to fulfill its authority over the Defence Security Program, close coordination with, and periodic reporting from, other functional authorities are required.

In addition to these organizational structure changes, it was recommended that governing bodies be established to support execution of the Defence Security Program. The Senior Security Advisory Committee (SSAC) was re-established as the advisory body to the DM and CDS, providing guidance and oversight on security matters affecting the Department. This Committee is chaired by the VCDS and supported by the DSO. Its responsibilities listed in the terms of reference[5] include the following:

- providing security risk management guidance and decisions to ensure that all security risks are documented, assessed, and treated as appropriate, commensurate with residual risk tolerance;
- ensuring that the results of security risk assessments are integrated within the Corporate Risk Profile to ensure alignment of security priorities with the Program Alignment

[2] Treasury Board Secretariat, Operational Security Standard: Management of Information Technology Security.
[3] Treasury Board Secretariat, Directive on Departmental Security Management, July 1, 2009.
[4] A functional authority sets standards, communicates clear expectations, and issues binding functional direction on behalf of the DM or CDS for an assigned area of responsibility. They also monitor to ensure compliance with direction and create a management framework whereby the DM or CDS can hold senior commanders and advisors across the organization accountable for compliance.
[5] Terms of Reference, SSAC, October 31, 2014.

Architecture, Report on Plans and Priorities, Departmental Performance Report, and other strategic plans or reports;

- providing collaborative leadership to ensure that appropriate security measures, risk mitigation strategies, and resources are in place for the effective and efficient management of security within the DND/CAF to include bringing security items of concern up through the chain of command for appropriate discussion and decision;
- reviewing the results of performance measurements, audits, and evaluations to identify areas for improvement and track progress towards the achievement of desired outcomes; and
- supporting the development and execution of the DSP.

Four sub-committees were also to be established with the responsibility to bring security concerns in their respective areas to the attention of the SSAC, including one specifically for IT Security.

The renewed focus on departmental security also resulted in the promulgation of several key documents. A new policy suite called the National Defence Security Orders and Directives was published in June 2015, superseding previous collections. The new suite of policies served to update security program authorities, roles and responsibilities for DGDS, Level Ones,[6] and all DND/CAF personnel. It also updated the departmental policy requirements across all security program elements including security risk management, information technology security, and oversight and compliance.

In addition, the first DSP was approved by the DM and CDS in May 2015, fulfilling the requirement of the Treasury Board Policy on Government Security (2009). The primary objectives of the DSP were to detail decisions for managing security risks, and to outline strategies, goals, objectives, priorities, and timelines for improving security over the next three years.

The process used to develop the DSP was documented and based on a security risk assessment methodology described as being consistent with Treasury Board Secretariat guidelines and the DND/CAF Corporate Risk Profile. Development of the DSP was the first attempt to gather and assess security risk information across the Department from program, security control objective area, and Level One perspectives. Based on this assessment, plans were required to address risk areas assessed as being above the accepted tolerance level. DGDS expects to provide periodic status reports on DSP implementation to the SSAC.

The DND/CAF have adopted the 15 Treasury Board-mandated security control areas applicable to all government departments, plus identity management, force protection and travel security for a total of 18 specific security control areas. IT security is one of the 18 security control objective areas. As part of the DSP development, ADM(IM) or subordinate organizations were identified as being responsible for implementing the risk treatment plans that addressed the DSP-identified

[6] Level One is defined as a senior official, either civilian or military, who has direct accountability to the DM or the CDS. (e.g., ADM(IM), Commander of the Canadian Army).

IT security risks. As a result of the Level One risk assessments, the DSP noted that IT security and/or information assurance risks affected most Level Ones. At least ten Level Ones outside ADM(IM) identified IT security-related risks and committed to implementing mitigation activities. Although not necessarily responsible for executing these activities, ADM(IM) was identified as having a secondary role to play in their implementation.

1.1.3 IT Security Program

ADM(IM) is responsible for establishing strategic direction and governance structures for all IM/IT activities, including IT security. While the DSO is the functional authority for the Defence Security Program, ADM(IM) is delegated the functional authority for IT security in the DND/CAF. The role of IT Security Coordinator for the Department is assigned to DIM Secur. According to the DND/CAF IT Security policy,[7] DIM Secur is responsible for the following:

- being the IT Security Coordinator and acting as the IT Security Authority in the Department;
- establishing and managing the IT Security Program as part of a coordinated Departmental Security Program; and
- serving as the principal IT security contact for the DND/CAF.

Consistent with TBS policy, departmental policy states that the IT Security Coordinator has a dual reporting relationship to the DSO (DGDS) and the Chief Information Officer (ADM(IM)). This relationship recognizes IT security as a crossing between the Security and IM/IT Programs. Adding complexity to the IT Security Program, Shared Services Canada also has responsibility for IT across the Government of Canada. Specific to IT security, Shared Services Canada is "mandated to protect the infrastructure and associated data in transit, storage, and use."[8] Shared authorities for security of DND/CAF assets increases the importance of a common understanding of security risks and tolerance levels. This common understanding should provide the basis for clear setting of priorities and ensuring activities and resources are aligned to appropriately manage security risks.

The primary governance body in place to support ADM(IM) in managing IM/IT activities in the DND/CAF is the Information Management Board (IMB). The IMB provides strategic leadership and recommends priorities on all matters related to the delivery and support of IM/IT in the DND/CAF. It also governs the corporate account used to record expenditures in support of department-wide IT systems and backbone services, and provides strategic advice and endorsements on major IM/IT activities, plans, and policies. It is co-chaired by ADM(IM) and VCDS/Chief of Programme. While SSAC membership includes ADM(IM), DGDS is not an IMB member given its mandate of managing IM/IT activities across the Department.

Until recently, various IT security stakeholders participated in the IT Security Coordination Working Group chaired by Chief of Staff (IM). Its terms of reference included identifying IT security risks and priorities and establishing and maintaining the Departmental IT Security

[7] Defence Administrative Order and Directive 6003-0 Information Technology Security, April 2012.
[8] Shared Services Canada website, Cyber and IT Security, http://www.ssc-spc.gc.ca/pages/cyber-eng.html.

Strategy and Plan. The IT Security Coordination Working Group was to report on these items to the IMB. However, this Working Group disbanded in January 2014 and was supposed to be replaced by the IT Security Committee. Although the terms of reference for this new committee were drafted, as of October 2015, they had not been approved, and the Committee had yet to be stood up.

It is anticipated that the IM/IT Programs will undergo changes under the Defence Renewal initiatives. These initiatives are being used, in part, to enhance the governance structure and strengthen ADM(IM)'s functional authority for the IM/IT Program.

1.1.4 IT Security Roadmap

One of the mechanisms ADM(IM) uses to issue direction is the Defence IM/IT Strategy. It was most recently released in October 2014 and outlined three strategic drivers: Success in Operations; a Secure, Reliable, Integrated Information Environment; and an Affordable and Sustainable IM/IT Programme. The IT Security Roadmap was initially drafted in June 2010 in support of the second strategic driver. It was refreshed by DIM Secur in March 2014 to provide an overview of the IT Security Program. The desired end state was a department-wide, coordinated, and prioritized list of activities ensuring that IT Security priorities were addressed in the most efficient and timely manner with minimal duplication.

The IT Security Roadmap has four objectives that reflect characteristics of an established IT Security Program. As such, it states that the Program should do the following:

1. follow the DND/CAF security framework;
2. be consistent with security policies and based upon standards;
3. provide for oversight that is exercised through a clear governance model consistent within the DND/CAF and across the Government of Canada; and
4. measure success of the Security Program.

These objectives are supported by forty-two distinct activities with milestone dates set between 2014 and 2024. Consistent with the Treasury Board Secretariat Operational Standard for the Management of Information Technology Security, the IT Security Roadmap activities are organized across four pillars: governance, people, process, and technology. Multiple departmental organizations are identified as having a role in executing IT Security Roadmap activities. They are as follows:

- ADM(IM) organizations: Chief of Staff (IM), Director General Information Management Operations, J6 Coordination, Canadian Forces Information Operations Group, Canadian Forces Network Operations Centre, Director General Information Management Technology and Strategic Planning, DIM Secur, and Director Information Management Engineering and Integration
- VCDS organization: Director General Cyberspace
- Canadian Forces Intelligence Command

Notably, all of these organizations are outside the purview of DIM Secur, and neither the DSO nor Shared Services Canada are reflected as being responsible, in full or in part, for any of the activities.

1.2 Objectives

The objective of the audit was to assess the governance and control practices in place to ensure implementation of the IT Security Roadmap.

1.3 Scope

The scope of the audit was the IT Security Roadmap (March 2014) and its progress up to September 2015. Shared Services Canada activities were excluded from this audit.

1.4 Methodology

The audit results are based on the following:

- interviews with DGDS staff and representatives from five ADM(IM) organizations including DIM Secur, which are responsible for executing the majority of the IT Security Roadmap activities;
- reviews of Government of Canada and departmental security policies; and
- reviews and analyses of key DND/CAF documents, such as the Corporate Risk Profile, DSP, Defence IM/IT Strategy, IT Security Roadmap, and terms of reference, agendas, supporting documentation, and records of decisions from key governance bodies.

1.5 Audit Criteria

The audit criteria can be found at Annex B.

1.6 Statement of Conformance

The audit findings and 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 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 and apply only to the entity examined.

2.0 Findings and Recommendations

2.1 IT Security Objectives and Priorities

The governance framework and supporting processes were not fully established to facilitate the identification of program level objectives and priorities required to mitigate IT security risks to an acceptable level.

Success of the IT Security Program relies upon establishing clear, measureable objectives and identifying priorities and activities that will effectively and efficiently address security risks and prioritized gaps in security controls. Establishing objectives and priorities is predicated on a governance framework that enables direction setting and decision making based on security risk information, existing controls, and a predetermined tolerance for residual risk. While the security program has seen significant changes to its governance structure, similar enhancements to the IT Security Program governance structure have not occurred.

2.1.1 Governing IT Security

While ADM(IM) is the functional authority for IT security, DIM Secur is the IT Security Coordinator and has the authority to establish and manage the IT Security Program as part of a coordinated Defence Security Program. DIM Secur is also identified as the primary contact for IT security in the DND/CAF. However, assigned IT security authorities have not been enforced or supported by an effective governance structure.

Good Practice

IT security authorities were defined and an IT Security Coordinator was appointed.

For example, DIM Secur was the lead organization responsible for developing the IT Security Roadmap. Although it was developed in March 2014, there was no evidence to demonstrate that IT security risks, objectives, priorities, or the IT Security Roadmap itself were discussed or formally approved. Despite DIM Secur's appointment as the IT Security Coordinator, staff indicated they did not have the authority to task other organizations, either within or outside ADM(IM).

Because the IT Security Roadmap was never formally approved, communicated, or tasked, not everyone was aware of its existence or that they were responsible for implementing the assigned activities. While the Roadmap was being developed by DIM Secur, other organizations with IT security responsibilities were also developing IT security-related plans without coordinating or explicitly aligning them with the IT Security Roadmap. For example, the DSP risk treatment plans referenced an "IT Security Roadmap" that was being developed by another directorate within ADM(IM). Multiple plans developed in silos by organizations with different responsibilities and visibility in the Department weaken the authority delegated to DIM Secur to establish and manage the IT Security Program and be the primary contact for IT security in the Department.

Good Practice

IT security was consistently identified as a priority area in key documents such as the DSP, the Defence Priorities document, the Defence Plan, the ADM(IM) Campaign Plan, ADM(IM) Functional Planning and Guidance document, and the IT Security Strategy.

The IT Security Committee, a sub-committee of the SSAC, has also not been stood up to provide clear and consistent direction and oversight in support of ADM(IM)'s authority for IT security. More than nine organizations outside of DIM Secur were identified as being responsible for implementing the activities in the IT Security Roadmap. Although all of the IT Security Roadmap activities were assessed as high priority, interviewed ADM(IM) representatives outside DIM Secur indicated that the activities did not necessarily reflect the priorities of their organizations. Organization priorities were directed from their respective chain of command, not as part of an IT Security Program. With DIM Secur unable to effectively exercise its authority and the IT Security Committee not yet established, there is a gap at the program level to horizontally assess IT security risks and provide clear direction on IT security to Level One organizations regarding objectives and priorities for implementing related activities across the Department.

2.1.2 Developing the IT Security Roadmap

The IT Security Roadmap lists four objectives and forty-two distinct activities. All forty-two activities were mapped to three of the four objectives. Each activity identified at least one responsible organization and a funding approach and had milestone dates spanning the period between years 2014 and 2024. None of the activities were linked to the fourth objective—performance measurement of the IT Security Program.

The process used to develop the IT Security Roadmap objectives, priorities, and activities was not defined, and it was unclear whether risk information was available, gathered, or used. Interviewees also consistently expressed concern that IT Security risk was not well understood or managed in the DND/CAF. As a result, it was unclear whether the IT Security Roadmap objectives, priorities, and activities responded to IT security risks identified at the time the Roadmap was developed or to new ones that have emerged since then.

Since 2013, the DND/CAF Corporate Risk Profile has set the risk tolerance level for security at medium but assessed the residual risk to be significant. In order to have an effect on the assessed residual risk level, program plans should have reflected the necessary actions to progress the Department towards the desired residual risk level (medium).Without an understanding of risks, current controls, and associated gaps, it is unclear how decisions to implement specific IT security activities were made and what impact their implementation was expected to have on the departmental security residual risk level.

The IT Security Roadmap should provide direction from the IT security authority and set a common foundation for allocating resources and for coordinating, monitoring, and reporting on implementation to ensure activities are executed. Interviewed representatives from organizations identified to execute the IT Security Roadmap were unclear on what the intended scope, outputs, and performance measures or expectations would be for the assigned activity. With unclear

expectations, there is no foundation for measuring, monitoring, or reporting on the performance of the IT Security Program, and the Department is not well positioned to ensure that the IT Security Roadmap activities will be implemented. In November 2014, DIM Secur created the IT Security Coordination Manager position and assigned the responsibility for developing performance measures that will be used to monitor and report on implementation of the IT Security Roadmap and the IT Security Program to it. At the time of the audit, IT Security performance measures were being developed in coordination with DIM Secur and two other ADM(IM) directorates—Director Information Management Engineering and Integration and Director Defence Information Management Planning.

2.1.3 Integrating Planning Processes

Planning processes for the IT Security Roadmap and DSP were not integrated. The IT Security Roadmap was developed prior to, and separate from, the DSP. The DSP development process included an assessment of identified security risks from the program, security control, and Level One perspectives.

As risk assessment processes used to develop the DSP mature and the Department's understanding of risk information improves, these could be leveraged to provide a higher level of assurance that IT security-related action plans are consistently prioritized to address identified risks. This would serve to ensure that the IT Security Program is aligned with the Defence Security Program, while also supporting the objectives and priorities of the IM/IT Programs. In addition, DIM Secur, as the IT Security Authority, could be relied upon to ensure that identified IT security risks in the DSP (at the levels of program, security control area, and Level One) are accurate. If planning processes are not coordinated and aligned, ADM(IM) risks losing the momentum and commitment required to use the IT Security Roadmap as its program level document to communicate, coordinate, monitor, and report on strategic direction.

2.1.4 Conclusion

Without the support of a clear and integrated IT Security governance framework, ADM(IM) and DIM Secur will continue to face challenges in effectively exercising their delegated authorities. Processes are needed to ensure that activities in the IT Security Roadmap are formally approved, communicated, or tasked to, and understood by responsible organizations.

Planning processes were not coordinated or based on a common understanding or assessment of security risk information. As a result, it was unclear whether objectives, priorities, and associated action plans addressed the highest IT security risks and prioritized gaps. Integrated and coordinated planning processes would provide a foundation for allocating resources based on affordability and impact on residual risk, while establishing a foundation for accountability for results.

ADM(RS) Recommendation

1. ADM(IM) should further develop the governance framework in support of exercising the functional authority for IT security across the DND/CAF.

OPI: ADM(IM)

Key considerations for development of a management action plan are as follows:

- In coordination with DGDS, ensure alignment and integration of IT Security Program objectives, priorities, and results with both the IM/IT and Security Programs and associated risk tolerance levels;
- Clear, consistent, and authoritative direction for action plans across the Department;
- Performance measures to articulate clear expectations;
- Establishment of the IT Security Committee; and
- Accountability for results.

ADM(RS) Recommendation

2. ADM(IM) should establish processes to define IT Security Program objectives and priorities within the context of the governance framework (to be developed) and identified risks.

Key considerations for development of a management action plan are as follows:

- Identify and enforce one focal point as the authoritative source for IT Security Program planning and management across the DND/CAF.
- Use the identified focal point to integrate the IT Security Program plans with other planning and reporting processes that may have different time horizons (e.g., functional planning guidance, fiscal year, business planning, and the DSP).
- Determine how threat and risk information will be gathered from internal and external environments, assessed (likelihood and impact), reported, and used to support decision making and adaptability of action plans.
- Establish the necessary links with other organizations that have essential information to ensure the IT security objectives, priorities, and plans are consistently understood and reflect DND/CAF and Government of Canada priorities, business and operational needs, and risk tolerance levels.

OPI: ADM(IM)

2.2 Implementation of IT Security Program Plans

Processes were not established to coordinate, monitor, and report holistically on IT Security Program objectives, priorities, and activities, and their impact on residual risk.

Execution of the IT Security Roadmap relies upon establishing processes to organize and guide the organizations responsible for implementing its activities. These processes should support effective management and accountability for the direction set through the governance

framework. They should also ensure that priorities and activities are resourced and executed, that risks are appropriately managed, and that organizations are held accountable for achieving established objectives and performance expectations.

2.2.1 Coordinating, Monitoring, and Reporting

> **Good Practice**
>
> DIM Secur recently allocated resources to coordinate, monitor, and report on the IT Security Roadmap.

Given that the IT Security Roadmap has not been formally approved, it is understandable that processes to coordinate, monitor, and report on the implementation of the IT Security Roadmap from a holistic perspective were not established or initiated. The IT Security Roadmap did not specifically articulate coordinating, monitoring, or reporting responsibilities or requirements. However, DIM Secur recognized this gap in fulfilling its delegated authorities for the IT Security Program and, as a result, an IT Security Coordination Manager section head position was established in November 2014. The IT Security Coordination Manager is responsible for developing the necessary processes (e.g., coordination, monitoring, and reporting) to support DIM Secur in managing the IT Security Program.

Assignment of activities from the IT Security Roadmap did not reflect the full extent of roles and responsibilities articulated in policies, particularly where coordination between stakeholders, including other Level Ones and Shared Services Canada, would be required. For example, the DSO was not assigned a role for any activity in the IT Security Roadmap despite being responsible for the overarching Security Program. Having said that, the structure of the Defence Security Program was approved just prior to the development of the IT Security Roadmap. Roles and responsibilities were being established and, as of October 2015, the IT Security Roadmap had not been revised to reflect these Program changes.

Monitoring and reporting of the IT Security Roadmap has been limited; there was no evidence that its implementation was monitored from a holistic perspective. However, agendas for the IMB—the IM/IT Program governance body—did include specific IT security projects that align with some of the activities under the technology pillar of the IT Security Roadmap. Records of decision indicate that the IMB briefings and discussions for these projects focused on their status and associated expenditures. While this focus aligns with the terms of reference for this body to govern the corporate account and provide strategic advice and endorsement of major IM/IT activities, there was no evidence that the IMB monitored the implementation of the IT Security Roadmap, a significant IM/IT plan and security plan, in its entirety.

In addition, as of October 2015, the IT Security Committee had not been established to support authoritative direction, ensure plans are actioned, and bring IT security concerns to the attention of the SSAC. Once established, the IT Security Committee could also challenge, leverage, and coordinate individual efforts across the Department, assess progress and performance of implemented measures, and reassess IT Security Program risks, gaps, and associated priorities.

2.2.2 Resources

The Treasury Board Secretariat Operational Security Standard: Management of IT Security requires departments to update their IT Security Action Plans and determine the resources required to implement them when deficiencies are identified and remedial actions are determined. The IT Security Roadmap included a recommended funding approach (i.e., Vote 1 or Vote 5) for each activity. It did not include cost estimates, confirmed funding sources, or identified resource gaps to be addressed in order to achieve planned milestones. DND/CAF IT security activities and associated resources are also not centrally managed. They are dispersed throughout the Department—across organizations, projects, and systems. There are no processes in place to horizontally review and prioritize departmental IT security activities or associated resources at the corporate, program, and system levels.

However, there are a number of opportunities to ensure that resources are aligned across the IT Security Roadmap. For example, the Defence Renewal initiative to rationalize the IM/IT Program started with identifying all IM/IT plans and expenditures. In addition, the DSP provides greater visibility of IT security action plans in ADM(IM) and across the Level Ones. There has also been an attempt to draw attention to, and fund, action plans that addressed security risks in the Department. At the strategic level, the Defence Plan (2015) directed Level Ones to fund their risk treatment plans from the DSP in their fiscal year 2016/17 business planning process. Finally, $12 million was approved as baseline funding for an IT Security Enhancement Program to address IT security risks and threats through technology solutions.

Although all of these events are independent of one another, they demonstrate an increased priority to fund security activities and to provide more central visibility of IM/IT plans and expenditures across the Department. The IT Security Program could benefit from these trends by horizontally reviewing and aligning departmental resources with prioritized activities.

2.2.3 Conclusion

With the number of organizations involved in the execution of the IT Security Roadmap, processes to horizontally coordinate efforts (including opportunities to leverage and ensure alignment of resources), monitor, and report on progress and results are a critical requirement. Creating the IT Security Coordination Manager position is a positive step in the horizontal coordination, monitoring, and reporting of processes. Without these processes, it will be difficult to align resources and assess progress or the impact that departmental efforts are having on the state of IT security in the DND/CAF. These processes should provide the information necessary to hold individuals accountable for implementation of activities and associated results relative to the expectations directed through the governance framework. The information could also be used to reassess security risks, objectives, and priorities for IT security in the DND/CAF.

ADM(RS) Recommendation

3. ADM(IM) should pursue the establishment of processes to horizontally coordinate, monitor, and report on the IT Security Program's objectives, priorities, and activities.

OPI: ADM(IM)

Key considerations for development of a management action plan are as follows:

- Clarify and enforce roles and responsibilities;
- Identify and leverage resources and efforts across the Department;
- Determine frequency and format of reports;
- Assess the impact of progress and performance on residual risk; and
- Identify circumstances and mechanisms to escalate areas requiring more attention or engagement from senior management (e.g., resources, residual risk levels).

ADM(RS) Recommendation

4. ADM(IM) should develop the accountability mechanisms, within the context of the governance framework for IT security (to be developed), to include progress, performance, and impact on residual risk at the corporate, program, and system levels.

OPI: ADM(IM)

3.0 General Conclusion

ADM(IM) has the functional authority for the IT Security Program and is supported by DIM Secur as the IT Security Coordinator. However, the Program would benefit from the necessary governance structure improvements and supporting management processes to do the following:

- provide clear, consistent, and authoritative direction;
- ensure departmental efforts and resources are coordinated and aligned horizontally with priorities; and
- monitor and report on progress and performance in relation to objectives and residual risk.

Without an effective governance framework and management processes, it is difficult to enforce direction, assign accountability, and ensure appropriate actions are being taken across the Department. The IT Security Program governance and control practices need to further evolve to support ADM(IM) in exercising the functional authority for IT security as part of a coordinated and maturing Defence Security Program. This will ensure that clear plans are developed, prioritized, resourced, and implemented to mitigate identified risks to an acceptable level.

Annex A—Management Action Plan

ADM(RS) uses recommendation significance criteria as follows:

Very High—Controls are not in place. Important issues have been identified and will have a significant negative impact on operations.

High—Controls are inadequate. Important issues are identified that could negatively impact the achievement of program/operational objectives.

Moderate—Controls are in place but are not being sufficiently complied with. Issues are identified that could negatively impact the efficiency and effectiveness of operations.

Low—Controls are in place but the level of compliance varies.

Very Low—Controls are in place with no level of variance.

IT Security Objectives and Priorities

ADM(RS) Recommendation (High)

1. ADM(IM) should further develop the governance framework in support of exercising the functional authority for IT security across the DND/CAF.

Management Action

1.1 ADM(IM) is undertaking an IM/IT Programme governance renewal effort under the mandate of Defence Renewal Initiative 3.3 – Rationalizing the Defence IM/IT Programme. This effort, which is in the implementation phase, is making coordinated changes to the overall IM/IT governance framework.

The IM/IT Programme governance renewal initiative will enable the departmental IT Security Authority. The IT Security Authority role has been integrated into the design of the IM/IT governance framework in multiple ways to ensure the following:

- IT security-related accountabilities, responsibilities, and authorities are clearly defined and articulated in the IM/IT policy framework;
- IT security requirements for the Defence IM/IT Programme can be captured and articulated;
- IT security activities are planned in coordination with all IM/IT activities;
- IT security perspective is included in the IM/IT capability development decision framework;
- IT security perspective is included in the architecture review process that includes verification of policy standards compliance; and
- IT security-related services are included in the service catalog and managed accordingly.

OPI: ADM(IM)
Target Date: March 2017

ADM(RS) Recommendation (High)

2. ADM(IM) should establish processes to define IT Security Program objectives and priorities within the context of the governance framework (to be developed) and identified risks.

Management Action

2.1 The Information Technology Security Committee (ITSC) will be established. Reporting to the SSAC, the ITSC will receive risk tolerance guidance from the SSAC and act as the prioritization authority for the IT Security Roadmap activities. This prioritization will be based on input from departmental risk assessments, security assessment and authorization results (risk register), results from the information system incident handling process, oversight and compliance reports, etc. The ITSC will provide linkage to the IM/IT IMB to ensure that IT security priorities align with overall DND/CAF IM/IT priorities.

OPI: ADM(IM)
Target Date: June 2016

Implementation of IT Security Program Plans

ADM(RS) Recommendation (Very High)

3. ADM(IM) should pursue the establishment of processes to horizontally coordinate, monitor, and report on the IT Security Program's objectives, priorities, and activities.

Management Action

3.1 ADM(IM) will refresh/update the IT Security Roadmap. The IT Security Roadmap requires update for submission to the ITSC. Following this refresh, DIM Secur D4 will maintain the document through direct coordination with the stakeholders.

OPI: ADM(IM)
Target Date: September 2016

3.2 The terms of reference for the Information Systems Security Exchange Forum will be reviewed and revised. The IT Security Roadmap groups activities under four pillars: governance, people, processes, and technology. The Forum's terms of reference require review to reflect that it will be the work group addressing governance, people, and process activities in support of the ITSC. With representation from stakeholders (working level), the aim of the Forum is to meet regularly to report on progress and identify issues requiring ITSC involvement.

OPI: ADM(IM)
Target Date: September 2016

3.3 The terms of reference for the Cyber Security Coordination Working Group will be reviewed and revised. The IT Security Roadmap groups activities under four pillars: governance, people, process and technology. The Working Group's terms of reference require review to reflect that it will be the work group addressing the technical activities in support to the ITSC. With

representation from all stakeholders (working level), the aim of the Working Group is to meet regularly to report on progress and identify issues requiring ITSC involvement.

OPI: ADM(IM)
Target Date: September 2016

3.4 Roles and responsibilities of DIM Secur D4 will be refined to be consistent with this management action plan. This role will include coordination with all stakeholders (Canadian Forces Intelligence Command, Canadian Forces Information Operations Group, DGDS, etc.) and integration with the DSP.

OPI: ADM(IM)
Target Date: April 2016

ADM(RS) Recommendation (High)

4. ADM(IM) should develop the accountability mechanisms, within the context of the governance framework for IT security (to be developed), to include progress, performance, and impact on residual risk at the corporate, program, and system levels.

Management Action

4.1 Roles and responsibilities of DIM Secur D4 will be refined. Working closely with the Roadmap activity stakeholders, DIM Secur D4 will assist them in establishing performance measures and will track progress and report to the ITSC and DIM Secur.

OPI: ADM(IM)
Target Date: April 2016

4.2 ADM(IM) will continue the implementation of the departmental Security Assessment and Authorization process and increase frequency of the risk register publication to quarterly as the tool to understand residual risk. The results expressed in the IT risk register will be used by the individual operational authorities to manage the system-level risks under their purview and by the DSO in documenting the overall departmental risks.

OPI: ADM(IM)
Target Date: November 2016

Annex B—Audit Criteria

Criteria Assessment

The audit criteria were assessed using the following levels:

Assessment Level and Description
Level 1: Satisfactory
Level 2: Needs Minor Improvement
Level 3: Needs Moderate Improvement
Level 4: Needs Significant Improvement
Level 5: Unsatisfactory

Governance

Criteria

1. Objectives and priorities are established and respond to identified risk.

   Assessment Level 4 – Objectives and priorities are unclear and do not respond to identified risk and corporate risk tolerance levels.

2. Objectives and priorities have been translated into specific activities that are assigned in alignment with roles and responsibilities for execution.

   Assessment Level 3 – The IT Security Roadmap objectives were translated into activities and milestones. Activity OPIs were not aware that activities had been assigned to their organizations. The assignment of activities from the IT Security Roadmap did not reflect the full extent of roles and responsibilities articulated in policy, particularly where coordination between stakeholders would be required.

3. IT security activities are coordinated to achieve objectives.

   Assessment Level 4 – To date, efforts to coordinate, monitor, or report on the implementation of the IT Security Roadmap from a holistic perspective has not been initiated.

4. Performance measurement and reporting expectations are defined, communicated, and fulfilled.

   Assessment Level 4 – Performance measurement and reporting expectations were not defined, communicated, or fulfilled. Processes are not established to communicate, task, coordinate, monitor, and report holistically on program objectives, priorities, and activities. The IT Security Roadmap did not include specific performance measures.

Sources of Criteria

Committee of Sponsoring Organizations of Treadway Commission, Internal Control – Integrated Framework, 2013

Canadian Institute of Chartered Accountants' Criteria of Control Framework, 1995

Treasury Board Secretariat**,** Audit Criteria Related to the Management Accountability Framework: A Tool for Internal Auditors**,** 2013
Reference to: AC-1, RM-4, RM-5, G-3, G-4, G-5, LICM-2, ST-1, ST-17, ST-18, ST-20, RP-1, RP-2, RP-3

Treasury Board Secretariat, Policy on Government Security, 2009
Reference to: Section 3.5, Section 6.1, Section 6.2

Treasury Board Secretariat, Directive on Departmental Security Management, 2009
Reference to: Section 3, Section 6.1.1.1, 6.1.1.4, 6.1.2, 6.1.4, 6.1.15, 6.1.22, 6.1.23, Appendix C

Treasury Board Secretariat, Operational Security Standard: Management of Information Technology Security
Reference to: Part 3, Section 12; Part 2, Section 9

Information System Audit and Control Association, *CoBIT 5 Framework, 2012*

National Institute of Standards and Technology, *Special Publication 800-53A, 2010*
Reference to: PM-4, PM-14