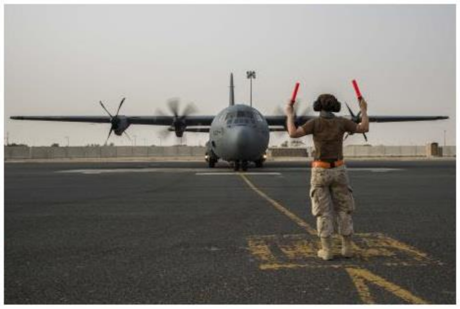
National Defence Défense nationale

ASSISTANT DEPUTY MINISTER (REVIEW SERVICES)

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

Evaluation of the Defence IM/IT Programme



Performance Measurement and Evaluation Committee

June 2020

1258-3-020 (ADM(RS))

Canada

Table of Contents

Acronyms and Abbreviations

ADM(Fin)	Assistant Deputy Minister (Finance)
ADM(IM)	Assistant Deputy Minister (Information Management)
ADM(Mat)	Assistant Deputy Minister (Materiel)
ADM(RS)	Assistant Deputy Minister (Review Services)
ADM(S&T)	Assistant Deputy Minister (Science & Technology)
ARA	Authorities, Responsibilities and Accountabilities
CA	Canadian Army
CAF	Canadian Armed Forces
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CBSA	Canada Border Services Agency
CID	Capability Investment Database
CIO	Chief Information Officer
Corp Sec	Corporate Secretary
C Prog	Chief of Programme
CTSAIS	Chief Technology and Security Architect for Information Systems
DAOD	Defence Administrative Orders and Directives
DGEAS	Director General Enterprise Application Services
DGIMPD	Director General Information Management Project Delivery
DIMEI	Director Information Management Engineering and Integration
DND	Department of National Defence
DRF	Departmental Results Framework
DRMIS	Departmental Resource Management Information System
ESA	Enterprise IT Service Agreement
FTE	Full Time Equivalent
FPG	Functional Planning Guide
FY	Fiscal Year
GC	Government of Canada
IM	Information Management
IMB	Information Management/Information Technology Program Management Board

IT	Information Technology
ITSM	IT Service Management
L1	Level One
NCR	National Capital Region
OCI	Office of Collateral Interest
OGD	Other government department
OPI	Office of Primary Interest
Op IT	Operational Information Technology
PAA	Performance Alignment Architecture
PAD	Project Approval Directive
RCAF	Royal Canadian Air Force
RCMP	Royal Canadian Mounted Police
RCN	Royal Canadian Navy
SLA	Service Level Agreement
SMC	Service Management Centre
SSC	Shared Services Canada
SSE	Canada’s defence policy: *Strong, Secure, Engaged*
TB	Treasury Board
TBS	Treasury Board Secretariat

Executive Summary

Purpose

This report presents the results of the evaluation of the Defence Information Management (IM)/Information Technology (IT) Programme, conducted between January 2018 and January 2019 by Assistant Deputy Minister (Review Services) (ADM(RS)) in compliance with the 2016 Treasury Board (TB) Policy on Results. As per the TB policy, the evaluation examines the relevance and performance of the program over a four year period, fiscal years (FY) 2015/16 through 2018/19.

The primary focus of the evaluation was on Departmental Results Framework (DRF) program 5.4 (IT Acquisition, Design and Delivery program) and DRF program 6.5 (Defence IT Services Program Management program).

Program Description

The Defence IM/IT Programme includes both IM and IT, whereby IT enables IM in support of the needs of the Defence Services Program. The activities related to DRF programs 5.4 and 6.5 produce information systems that support Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR). The Assistant Deputy Minister (Information Management) (ADM(IM)) is the functional authority accountable for the management of IT in the Department of National Defence/Canadian Armed Forces (DND/CAF) and is also the Defence Chief Information Officer (CIO) accountable to the Deputy Minister. The Defence CIO issues policy, direction and guidance to Level One (L1) organizations, and ensures that the activities of all IT service providers are coordinated in the delivery of integrated IM/IT capabilities that satisfy the needs of Defence services, including support to CAF operations.

Overall Assessment

- The Defence IM/IT Programme remains relevant and is consistent with the roles, responsibilities, priorities and objectives of the federal government and DND/CAF.
- The Defence IM/IT Programme would benefit from improving its communication strategy which would address issues such as awareness of new or updated policies among service providers.
- Due to numerous challenges faced, such as the ability to deliver on time, the Defence IM/IT Programme has undertaken a number of initiatives to improve the agility of IT projects delivered.
- The evaluation noted that delays in IT services provided by Shared Services Canada (SSC) have resulted in ineffective and slow support to operations.

Program deliverables include: applications, networks, and architectures; system management technologies; security technologies; and distributed technologies. The program objectives contribute both to operational and other shared capabilities required to enable Defence capabilities.

On August 4, 2011, the Government of Canada (GC) created SSC to transform how the Government manages its IT infrastructure; consequently, some services are now their responsibility. During FY 2012/13, following two Orders-In-Council, DND/CAF transferred certain IT responsibilities and resources to SSC.

Relevance

There is a continuing need for the Defence IM/IT Programme. IM/IT assets are critical to both the success of CAF military operations and training activities, as well as the corporate activities that support them. Operationally, information systems produced by the Defence IM/IT Programme enable C4ISR activities. This allows commanders to have information and decision superiority by being able to collect and disseminate the most relevant and accurate information in a timely and secure manner. Force Generators and Force Employers were unanimous in their reliance on IM/IT to train and conduct operations.

The Defence IM/IT Programme is in alignment with governmental and departmental priorities. One responsibility of the Defence CIO is to ensure that all departmental IM/IT activities coordinate with DND/CAF priorities. ADM(IM) is accountable for eight initiatives identified in Canada’s defence policy: *Strong, Secure, Engaged* (SSE) and is responsible to implement SSE-driven initiatives from other L1s.

Performance

Effectiveness

Future force capabilities leading to IT solutions evolve from a capability gap through to an IT requirement and eventually to project deliverables. Some difficulties experienced are in relation to insufficient information and/or a lack of mutual understanding and agreement on how the process works between project sponsors and the Defence IM/IT Programme’s intake process. The evaluation concluded that for IT projects, this process has worked; however improvements could be made. Several improvements to the Defence IM/IT Programme intake process are being considered, including a plan to set up an Information Design Authority board to look at investments by both major and minor projects.

The evaluation noted discrepancies in relation to the understanding of authorities, responsibilities, and accountabilities (ARA) delineation. In addition, the status of a revised governance model (the CIO Model) has remained unclear among service providers.[1] Likewise, unawareness of new or updated policies produced by the Defence IM/IT Programme among service providers and other stakeholders is also linked to communication challenges. Going forward, developing a communication plan would assist in strengthening the effectiveness of the program.

Enforcement of policies is another challenge that the Defence IM/IT Programme faces. There is no mechanism to ensure that stakeholders align themselves with the Defence IM/IT Programme's strategies. Evidence from interviews indicated that this is a known issue within the program, which does not have the capacity to force compliance or impose repercussions for those who do not comply with guidance and direction outlined in the Functional Planning Guidance (FPG). Both senior program officials and service providers acknowledge that once the CIO Model comes into greater effect, stakeholders will have no other option but to comply with the Defence IM/IT Programme's requirements in order to ensure that its own organizational needs are fulfilled.

Overall, the evaluation believes that deciding upon a governance model and fully committing to its complete implementation would ensure improved governance of the Defence IM/IT Programme. The current approach greatly hinders its capacity to enable effective governance.

Due to numerous challenges faced, such as the ability to deliver on time, the Defence IM/IT Programme has undertaken a number of initiatives to improve the agility of IT projects delivered. For example, the continuous intake process will allow "urgent/time sensitive" requirements to be approved more quickly.

The evaluation noted that delays in IT services provided by SSC sometimes resulted in ineffective and slow support to operations. Some of these delays stemmed from a lack of a service level agreement (SLA) between DND/CAF and SSC. As a result, monitoring of service quality and standards has been difficult.

Economy and Efficiency

The evaluation was unable to determine the actual cost of the program. Expenditure tracking has remained a challenge, and the Defence IM/IT Programme has limited visibility for at least half of Departmental IT expenditures. Based on the Treasury Board Secretariat (TBS) IT Expenditure Report,[2] net of exclusions, the program cost was $712,539,316 (2017/18). Costing difficulties were also noted in the 2016 evaluation of the Information Systems Lifecycle Program. A performance measurement strategy combined with improved expenditure tracking could alleviate the observed issues.

[1] Service providers include the Environmental Commands, Assistant Deputy Minister (Materiel) (ADM(Mat)) and Assistant Deputy Minister (Science & Technology) (ADM(S&T)).
[2] The IT Expenditure Report is submitted to TBS by each department annually to capture all IT related costs.

Not having an approved SLA with a clear delineation of roles and responsibilities between the Defence IM/IT Programme and SSC has continued to be problematic. This issue was also noted in the 2016 evaluation of the Information Systems Lifecycle Program. Without a complete costing model, this evaluation was unable to identify any savings in Defence IM/IT Programme expenses resulting from the transfer of services to SSC, and could not accurately presume future savings.

One of the initiatives of SSE[3] concerns improving defence procurement and aims "to reduce project development and approval time in the Department of National Defence by at least 50 percent for low-risk and low-complexity projects." It is believed that this process will improve overall efficiency.

Key Findings and Recommendations

Key Findings	Recommendations
Relevance	
1. There is a need for a Departmental Defence IM/IT Programme to provide essential support for CAF operations.	
2. The Defence IM/IT Programme is consistent with the roles, responsibilities, priorities and objectives of the federal government and DND/CAF.	
Performance – Effectiveness	
3. IM/IT requirements align with future force capabilities.	
4. There is a lack of understanding/agreement between project sponsors and the Defence IM/IT Programme's intake process over the prioritization of IT operational requirements versus other IT enterprise requirements.	1. Review the process and prioritization methodology for requirements used by the Defence IM/IT Programme Intake Process in collaboration with stakeholders to further clarify/promote transparency.
5. The Defence IM/IT Programme's lack of an effective communication strategy has hindered its ability to exercise governance and implement policy.	2. To strengthen governance and oversight of the Defence IM/IT Programme, ADM(IM) should: a. Establish and formalize Defence IM/IT ARAs. b. Review and consolidate Defence IM/IT policies to ensure alignment with established ARAs.
6. Within DND/CAF, the effectiveness and status of the revised IM/IT governance model remains unclear which is compounded by the lack of clearly defined ARAs.	

[3] SSE, initiative number 94.

7. Numerous policies and related documentation remain in draft format, making it difficult for service providers to ascertain the approval status of policies. This is further challenged by an inability for enforcement and inconsistent dissemination of policies and related documentation.	c. Establish a communication strategy to ensure that ARAs, policies, guidance and directives are disseminated holistically to stakeholders in DND/CAF.
8. Improvements are currently underway to enhance processes as the Defence IM/IT Programme finds it challenging to keep up with and incorporate evolving technologies in its delivery of systems, products and services.	
9. IT support provided by service management centres is inconsistent across DND/CAF, despite the establishment of SLAs by the Defence IM/IT Programme.	See recommendation 2.
10. Delays in IT services provided by SSC have resulted in ineffective and slow support to operations.	
11. Until the SLA between DND/CAF and SSC is signed, the monitoring of service quality and standards will be difficult.	
Performance – Economy	
12. This evaluation is currently unable to determine the actual cost of the program. Expenditures tracking remains a challenge, and the Defence IM/IT Programme has limited visibility for at least half of Departmental IT expenditures.	3. As part of the implementation of the revised governance model, ensure accurate attribution and tracking of expenditures throughout the Defence IM/IT Programme with links to the performance framework.
Performance – Efficiency	
13. There exists a duplication of systems, networks and efforts. The creation of Chief Technology and Security Architect for Information Systems (CTSAIS) and the Chief Application Architect aim to reduce these and enhance system integration.	
14. There are enhancements currently being implemented to improve project management and delivery.	
15. Until a complete costing model between DND and SSC is signed, this evaluation is unable to identify any savings in the Defence IM/IT Programme expenses resulting from the transfer of services to SSC, and cannot accurately presume future savings.	

Note: Please refer to Annex A—Management Action Plan for the management responses to these recommendations.

1.0 Introduction

1.1 Context for the Evaluation

This report presents the results of the evaluation of the Defence IM/IT Programme, conducted between January 2018 and January 2019 by ADM(RS) in compliance with the 2016 TB Policy on Results which requires departments to "measure and evaluate performance and use the resulting information to manage and improve programs, policies and services." As per the TB policy, the evaluation examines the relevance and performance of the program over a four year period, FYs 2015/16 through 2018/19. This report was conducted in accordance with the DND/CAF Five-Year Departmental Evaluation Plan. The findings and recommendations in this evaluation may be used to inform management decisions related to program delivery and resource allocation, and will serve as a baseline for future evaluations.

The Defence IM/IT Programme encompasses all IM and IT related activities undertaken within DND/CAF. It is sub-divided into seven programs spread across six Core Responsibilities within the DRF[4] delivered by ADM(IM), plus activities in other DRFs delivered by other L1 organizations. The primary focus of the evaluation was on DRF program 5.4 (IT Acquisition, Design and Delivery program) and DRF program 6.5 (Defence IT Services Program Management program), except where necessary to refer to the program in its entirety. Other DRF programs will be the subject of future evaluations. There have been previous evaluations and audits related to the Defence IM/IT Programme by ADM(RS) as follows:

- Evaluation of the Information Systems Lifecycle Program[5],[6] (2016);
- Audit of Information Technology Security: Roadmap Implementation (2015);
- Audit of IM/IT Framework to Support Transition to SSC (2015); and
- Audit of Application Access Rights (DRMIS) (2016).

[4] Defence IM/IT activities are embedded in the following DRF program areas:
1.5 Cyber Operations
2.6 Ready Cyber Forces
4.6 Cyber and Command Control
5.4 Defence IT Systems Acquisition, Design and Delivery
6.5 Defence Information Technology Services and Programme Management
7.6 Information Management Services
7.7 Internal Services - Information Technology Services.

[5] The Information Systems Lifecycle Program evaluation was conducted in alignment with the Performance Alignment Architecture (PAA)– the forerunner to the DRF.

[6] PAA 4.4.1, 4.4.2, 4.4.3, and 4.4.4.

1.2 Program Profile

1.2.1 Program Description

DND/CAF relies on a wide variety of IM/IT technologies in the conduct of day-to-day departmental business and in the conduct of military operations. The Defence IM/IT Programme includes both IM and IT, whereby IT enables IM in support of the needs of the Defence Services Program.[7] IT that is employed in the direct support of military operations is referred to as Operational IT (Op IT). While the Defence IM/IT Programme does not include Operational Technology (technology that is embedded within Defence platforms, equipment and/or infrastructure),[8] it does set the policies, standards and architectures for the interaction between Operational Technology and the Defence IM/IT Programme.[9]

The activities related to DRF programs 5.4 and 6.5 produce information systems that support C4ISR. Their expected outcomes are provided in the Logic Model in Annex C. The ADM(IM) is the functional authority[10] accountable for the management of IT in DND/CAF.[11] Further, as the Defence CIO,[12] the ADM(IM) ensures that the activities of all IT service providers are coordinated in the delivery of integrated IM/IT capabilities that satisfy the needs of Defence services, including support to CAF operations.[13]

The objective of DRF program 5.4 (Defence IT Acquisition, Design and Delivery) is to acquire, design, build and deliver IT and Op IT information systems and applications which have received funding in support of future force capabilities and enhancement. Key project phases in meeting this objective are definition and implementation. The definition phase of a project marks the transition from determining what should be done to mitigate a deficiency, to determining how the preferred option will be implemented. Projects that are approved move into the implementation phase where the focus is to deliver the project within the approved scope, cost, and schedule limits.

The objective of DRF program 6.5 (IT Services and Program Management) is to lead the Department in the planning, development, delivery, and support of innovative IM/IT

[7] Defence IM/IT Programme Definition. February 19, 2016.

[8] In the context of the Defence IM/IT Program, Operational Technology refers to technology (hardware and/or software) that is embedded within and/or core to the function of defence platforms, equipment and/or infrastructure. For example, an aircraft is comprised of numerous Operational Technologies such as control, sensor and weapon systems. The interface that enables the transmission of data into a network is referred to as Op IT.

[9] For additional detail and examples, see the document “Defence IM/IT Programme Definition” February 19, 2016.

[10] The ADM(IM) has functional authority in accordance with the Defence Administrative Orders and Directives (DAOD)1000-6, Policy Framework for Information Technology Management and DAOD 1000-8, Policy Framework for Safety and Security Management Document. In addition, ADM(IM) works under the guidance of the documents issued by other departments, e.g., TBS, SSC, and the Communications Security Establishment (CSE).

[11] Defence IM/IT Strategy 2016, ADM(IM).

[12] The role of Departmental CIOs as defined in the GC policy framework for IM and IT management and the role of ADM(IM) as the Defence CIO as defined in the DND/CAF policy framework (DAOD 1000-0, 6000 series).

[13] Defence CIO Model, DM Presentation, February 12, 2018, ADM(IM).

capabilities that enable successful Canadian Forces Operations and the achievement of DND and GC objectives. Activities within DRF program 6.5 include management of the existing IT services and management of the entire Defence IM/IT Programme including operations, maintenance, and support of existing IT services performed by service providers. Defence IM/IT Programme management activities are performed by the Defence CIO.

The Defence IM/IT Programme activities are delivered by service providers distributed across a number of L1 organizations, each of which has resource management authority over its own IT resources (see section 1.2.3).

Systems produced by the program include: applications, networks, and architectures; system management technologies; security technologies; and distributed technologies. The program objectives contribute both to operational and other shared capabilities required to enable Defence capabilities.

On August 4, 2011, the GC created SSC to transform how the Government manages its IT infrastructure; consequently, some services are now their responsibility. During FY 2012/13, following two Orders-In-Council,[14] DND/CAF transferred certain IT responsibilities and resources to SSC.[15] The IT activities that were transferred include delivering email, data centres, network services, as well as the purchase of IT equipment and its maintenance.

The IM/IT Programme Management Board (IMB) is the senior governance body for the Defence IM/IT Programme, co-chaired by the Defence CIO and Chief of Programme (C Prog). The IMB makes decisions regarding sustainment of and changes to the Defence IM/IT Programme strategies, priorities and activities. The IM Program Working Group supports IMB by providing a forum for consultation and collaboration on all matters related to the Defence IM/IT Programme activities (projects, initiatives and service delivery) in DND/CAF.

1.2.2 Program Background

Since 2006, DND/CAF has launched a series of transformations of the Defence IM/IT Programme:

- In 2006, the implementation of the IM Service Transformation began a centralization of all IM/IT services. Despite very significant initial work (moving

[14] The term “order-in-council” refers to a legal instrument generated by the Governor-in-Council and constitutes a formal recommendation of Cabinet that is approved and signed by the Governor General. Orders-in-council address a wide range of administrative and legislative matters including transactions between departments. (Source: Canada. Library and Archives Canada. *Databases: Orders in Council.* Online: 2016. http://www.bac-lac.gc.ca/eng/discover/politics-government/orders-council/Pages/orders-in-council.aspx. Consulted on July 25, 2016).
[15] Total resources transferred to SSC by DND/CAF were approximately $318 million and 761 positions (538 civilian and 223 military) to SSC.

$450 million and approximately 1,800 Full Time Equivalents (FTE), efforts stopped in 2008 with the announcement of the pending formation of SSC in 2011;

- In 2011, DND/CAF transferred $318 million and 761 positions (538 civilian and 223 military) to SSC;
- Following the Defence Renewal Team initiatives in 2013,[16] the number of service desks was reduced from approximately 122 to 22 with a goal to reassign staff and optimize IT service delivery;
- Consolidation of applications has taken place with a goal to both eliminate underused or duplicate applications as well as to optimize migration to common enterprise platforms; and
- Transformation efforts have also continued in evolving the governance model from a decentralized model to the planned CIO/Hybrid Federated model. In the decentralized model, the Defence IM/IT Programme holds approximately 49 percent of the total IM/IT expenditures with limited influence over the remainder. This is based on costs attributed to IT elements within Departmental Resource Management Information System (DRMIS). In the CIO/Hybrid Federated model, however, the Defence IM/IT Programme controls the majority of the total IM/IT expenditures but does not own all of the IM/IT systems and personnel. Currently, IM/IT expenditures and activities are managed locally, but reported centrally.

1.2.3 Stakeholders

The stakeholders of the Defence IM/IT Programme can be divided into the following categories:[17]

- Service Providers: An IM/IT service provider is any organization that employs IM/IT staff in the delivery of IM/IT capabilities. This includes: 14 L1 organizations; 4 Other Government Departments/Agencies;[18] 2 other governments/defence organizations[19] and third party contracted service providers;
- Policy Drivers: An IM/IT policy driver is any organization that sets policies, issues direction or sets conditions that directly or indirectly shape the Defence IM/IT Programme. For example, Vice Chief of the Defence Staff (C Prog) issues direction/policy on the project approval process (inclusive of IM/IT projects).
- IM/IT end-users: An IM/IT end-user is any organization that uses IM/IT services to conduct its business. Every DND/CAF organization is an IM/IT end-user.

[16] http://www.forces.gc.ca/en/about-reports-pubs-audit-eval/271p7055-64.page.

[17] Defence IM/IT Programme Definition, ADM(IM), February 19, 2016.

[18] Department of Foreign Affairs, Trade, and Development; Royal Canadian Mounted Police; SSC; Canadian Security Establishment.

[19] Department of Defence (United States); North Atlantic Treaty Organization.

The role(s) of a given stakeholder are used to determine how that organization interacts with the Defence IM/IT Programme. For example, while ADM(Mat) is an end-user of IM/IT services, it also delivers IM/IT through the capital program and is an IM/IT policy authority in the areas of procurement and minor capital projects.

1.3 Evaluation Scope

1.3.1 Coverage and Responsibilities

As described in Section 1.1, the evaluation focused on the performance of the program in the three following areas:

- whether the Defence IT requirements were aligned with future force capabilities;
- the effectiveness of the governance model of the program; and
- the impact of the transfer of services to SSC, from an operational point of view.

This included all activities charged to DRF program 5.4. Defence IT Systems Acquisition, Design and Delivery and DRF program 6.5 Defence Information Technology Services and Programme Management.

The evaluation did not assess the following activities:

- Management of corporate IT services (such as the DRMIS and the Human Resources Management System);
- IT security;
- Cyber security;
- Regional IT services provided to bases; and
- IT support to operations, (which was assessed in the Information Systems Lifecycle Program Evaluation, 2016).

Although the evaluation did not assess IM Operations, the evaluation considered the interface between operational service providers and ADM(IM), as well as the impact of operations due to the transfer of responsibilities to SSC.

1.3.2 Resources

In FY 2017/18, the Defence IM/IT Programme expenditures were $712,539,316.[20] For a more complete discussion of the Defence IM/IT Programme expenses, see discussion following Key Finding 12.

[20] DND TBS IT Expenditure Report, FY 2017/18.

1.3.3 Issues and Questions

In accordance with the TB Directive on Results (2016), the evaluation addresses issues related to relevance and performance. The methodology used to gather evidence in support of the evaluation questions can be found in Annex B. A logic model providing a theory of change for this program is included in Annex C. An evaluation matrix, listing each of the evaluation questions with associated indicators and data sources is provided in Annex D.

2.0 Findings and Recommendations

2.1 Relevance

Key Finding 1: There is a need for a Departmental Defence IM/IT Programme to provide essential support for CAF operations.

IM/IT assets are critical to both the success of CAF military operations and training activities, as well as the corporate activities that support them. Operationally, information systems produced by the Defence IM/IT Programme enable C4ISR activities. This allows commanders to have information and decision superiority by being able to collect and disseminate the most relevant and accurate information in a timely and secure manner. Force Generators and Force Employers were unanimous in their reliance on IM/IT to train and conduct operations. As one Force Employer stated "without information supremacy, we will fail." Corporately, the Defence IM/IT Programme provides the essential backbone applications and networks that permit every member of the defence team to provide information and make decisions that are important to support military operations and to fulfill obligations to safeguard information assets.

Demand for the products and services produced by the program has also remained high. Major and minor projects managed by all service providers within the Defence IM/IT Programme deliver technological solutions that directly enable existing military capabilities and/or fill capability deficiencies. The Defence IM/IT Programme, for example, manages an average of 20 major capital projects a year worth approximately $2.28 billion that provide capabilities for use by stakeholders across the department.

> *"We cannot work without the services provided by the ADM(IM) Group."*

Key Finding 2: The Defence IM/IT Programme is consistent with the roles, responsibilities, priorities and objectives of the federal government and DND/CAF.

The TBS CIO Branch has been assigned the role of functional authority for IM/IT at the federal level, and issues policy, directives and associated standards in the areas of IT governance and IT strategies to all federal departments.[21] The TBS Policy Framework for Information and Technology, dated July 1, 2007, assigns Deputy Heads responsibility for the effective management of information and technology in their Departments. In DND/CAF, the ADM(IM) is the Defence CIO and is accountable to the Deputy Minister for management of the Defence IM/IT Programme. In the role of functional authority for Defence IM/IT management, the Defence CIO issues policy, direction and guidance to L1s. The associated ARAs are described in the DND/CAF Organization and Accountability

[21] For example, TBS issued a Directive on Management of Information Technology (2009) to provide guidance to ensure that departmental programs are consistent with IT management processes across the GC.

document and the specific application of the functional authority is detailed in Defence Administrative Orders and Directives (DAOD) 6000 series policy framework forming the basis for IT governance and management in the department. The development of an annual departmental IT plan is also required by TBS and further ensures alignment with GC direction. To fulfill TBS mandated requirements, the Defence IM/IT Programme goes through an annual process of analyzing and validating planned IT spending of all L1s to ensure continued alignment across the department.

The Defence IM/IT Programme is in alignment with governmental and departmental priorities. One responsibility of the Defence CIO is to ensure that all departmental IM/IT activities coordinate with DND/CAF priorities. Of the 111 initiatives contained in SSE, ADM(IM) is the Office of Primary Interest (OPI) for eight and an Office of Collateral Interest (OCI) for an additional 27. Within the DRF, seven of the 64 DRF programs are the responsibility of the Defence IM/IT Programme. The Defence IM/IT Programme is also guided by the GC Strategic Plan for IM and IT 2017-2021, which identifies priorities and key activities. The program also aligns with priorities set by the departmental Information Management Board.

ADM(IM) is accountable for eight SSE initiatives,[22] such as Initiative 62 - Acquire joint command and control systems and equipment, specifically for integrated information technology and communications, and Initiative 63 - Acquire joint signals intelligence capabilities that improve the military's ability to collect and exploit electronic signals intelligence on expeditionary operations. In addition, the Defence IM/IT Programme is responsible to implement SSE-driven projects sponsored by other L1s.

2.2 Performance—Achievement of Expected Outcomes (Effectiveness)

2.2.1 Future Force Capabilities

Finding 3: IM/IT requirements align with future force capabilities.

Finding 4: There is a lack of understanding/agreement between project sponsors and the Defence IM/IT Programme's intake process over the prioritization of IT operational requirements versus other IT enterprise requirements.

Difficulties have stemmed from not having a sufficient voice in decision making and/or a lack of mutual understanding and agreement on how the process works between project sponsors[23] and the Defence IM/IT Programme, although the process for intake

[22] ADM(IM) is OPI for SSE Initiatives: 62, 63, 65, 68, 87, 88, 89, and 90.

[23] Project sponsors include organizations that submit capability requirements with IT components to the Defence IM/IT Programme prioritization process for design and implementation.

into the IM/IT programme is well documented and communicated across the governance structure. Future force capabilities leading to IT solutions evolve from a capability gap through to an IT requirement and eventually to project deliverables. The evaluation concluded that for IT projects, this has worked; however improvements are needed.

Future force capabilities that translate into IT requirements follow one of three paths. On one path are the Defence IM/IT Programme's minor capital IT procurement projects, and on the second path, DND/CAF equipment major capital procurement. The third path, shadow IT, is where the L1 has the funds and capacity to procure for themselves. IT procurement that is considered a major capital project[24] is included in the procurement and prioritization process with all other major capital purchases for consideration in the overall Defence Capability Plan. On the other hand, business intake for IT-related minor capital projects[25] are collectively considered and prioritized by the Defence IM/IT Programme through its governance and intake process.

Response to demand for the Defence IM/IT Programme is not limited to minor capital projects or procurement. The supply side, to meet that demand, is governed by the IM/IT Capability Development Board which may result in various ways to meet the demand, (e.g., minor projects, major projects, other service providers).

Major IT projects submitted to the Defence Capabilities Board are considered and prioritized in competition with non-IT major capital projects. This is viewed as a strong disadvantage by IT stakeholders as non-IT projects are not a part of the Defence IM/IT Programme's governance structure and therefore considered in isolation from the minor capital IT projects. This can lead to a lack of coordination between projects. This also means that IT major capital projects compete for funding against non-IT projects and initiatives.

Three challenges of prioritization factors, process issues and lack of understanding of process and requirements were noted. There is a widely-held belief among project sponsors that long-term enterprise requirements are viewed more favourably than operational requirements in the prioritization process. Some project sponsors feel that they do not have an adequate voice in the prioritization deliberations. They feel that the process is too controlled by the central programme staff and appears self-referential where they mandate the controls for themselves. Senior program managers underlined the lack of understanding of process and requirements noting that there was a need for increased knowledge by sponsors of how submissions should be prepared and presented.

[24] Normally greater than $5 million.

[25] Normally less than $5 million.

Senior program management expressed challenges that exist with establishing IT requirements with major capital projects. Two senior program managers noted that large projects that deliver capabilities that are not specifically IT-related do not always consider IT implications and therefore IT-requirement gathering is completed quickly and generally later in the process. This may result in the delivery of a capability that is not meeting the intent of the operator. The evaluation noted a recommendation among interviewees that Director General Information Management Project Delivery (DGIMPD) needs to become involved sooner because some activities that were once being done in later phases are now being done in earlier phases of the project. Furthermore, the rigidity of the financial framework forces them to have more information about the project (financially) at an earlier point. The timing of the release of funds has challenged their capability to address these issues. This has been seen in some of the SSE initiatives moving slower because they do not have the funding information necessary to move the project to a Vote 5[26] funding level. For example:

- Two space programs related to SSE 17 are suffering a 12-15 month delay getting to Project Definition; and
- Two Cyber projects are suffering a similar six month delay.

Several improvements to the Defence IM/IT Programme intake process are being considered or have already been instituted, such as:

- The Defence IM/IT Programme is considering separate prioritized lists in various categories with prioritization and funding for each;
- There is a plan to set up an Information Design Authority board to look at investments by both major and minor projects;
- A continuous intake process has been instituted to improve flexibility and to answer in-year operational requirements; and
- Work is underway to provide the Defence IM/IT Programme governance model with visibility of both Vote 1 and Vote 5 IT funding.

ADM(RS) Recommendation

1. Review the process and prioritization methodology for requirements used by the Defence IM/IT Programme Intake Process in collaboration with stakeholders to further clarify/promote transparency.
OPI: ADM(IM)

[26] "The majority of the Department's spending is comprised of Vote 1 and Vote 5 appropriations. Vote 1 funding is used to pay for operations and maintenance and includes the costs of using and maintaining equipment and infrastructure, communication, and professional services. Vote 5 funding is expended primarily for the acquisition of capital equipment, information systems, and infrastructure." (Source: Canada. Department of National Defence. Implementing Vote 1/Vote 5. Online: http://cfo-dpf.mil.ca/assets/FinCS_Intranet/docs/en/learning-careers/ndcc-implementing-vote-1-vote-5-2017-2018.ppt. Consulted on January 14, 2019).

2.2.2 Governance Strategy

Key Finding 5: The Defence IM/IT Programme's lack of an effective communication strategy has hindered its ability to exercise governance and implement policy.

Opinions on effective lines of communication within ADM(IM) as well as those with external stakeholders in DND/CAF are mixed. Interviews with senior program managers have suggested that communication levels were satisfactory, while comments from service provider organizations found that communication levels were insufficient. As a result, the Defence IM/IT Programme has had difficulty effectively sharing its initiatives and policies with other organizations within DND/CAF.

Internal to ADM(IM), senior program staff stated that they regularly meet with each other to ensure that there are no overlaps, that gaps are filled, and to break down silos under their authority. However, other program staff have stated that there needs to be better internal dialogue, and that there is a breakdown of communication as it goes farther down the chain of command. During interviews, some senior program managers agreed in this regard, stating that there is room for improvement with communication.

External to ADM(IM), 52 percent of service provider questionnaire respondents found that their organization did not have sufficient levels of communication with ADM(IM). The Defence IM/IT Programme established a number of committees designed to enable communication as part of the IT requirement intake process: the IM/IT Programme Management Board; the IM/IT Programme Working Group; the IM/IT Capability Development Board; the IT Service Design Working Groups; the IT Service Management (ITSM) Steering Committee; and, the IT Operations Committee.[27] However, comments from interviews and questionnaires revealed that due to committee attendance often being delegated downwards, the committees are usually attended by the same individuals, thereby limiting their effectiveness as a communication tool. Comments from interviews with senior program management have highlighted that there is a need to improve coordination between ADM(IM) and other service providers within the Defence IM/IT Programme. This coincides with comments from the service provider questionnaire, which has indicated that the Defence IM/IT Programme's objectives are not always clear and concise.

Senior program management acknowledged that the Defence IM/IT Programme needs to establish a communication campaign plan. Program managers have stated that multiple communication methods should be explored to reach the various audiences of DND/CAF.

[27] The IT Service Design Working Groups are partially in place and the IT Operations Committee is not yet in place.

Key Finding 6: Within DND/CAF, the effectiveness and status of the revised IM/IT governance model remains unclear which is compounded by the lack of clearly defined ARAs.

Impact of the CIO Model

While the CIO Model is in its early phases, the evaluation is unable to attribute improved program performance as a result of this governance model. As discussed in the introduction, the Defence IM/IT Programme proposed a new governance model which would evolve Defence IM/IT governance from a decentralized model to a CIO-hybrid federated model. The objective of this model is to improve the Defence IM/IT Programme's governance through increased oversight and control of IM/IT expenditures and activities.[28] However, there appears to be a disconnect between service providers regarding the preferred degree of this shift. Seventy-nine percent of service provider respondents to the questionnaire preferred a decentralized model of governance concerning the Defence IM/IT Programme's control over IM/IT expenditures. This indicates that service providers are not in favour of increased centralization of Defence IM/IT, which could impact the effectiveness of the CIO Model as it is implemented. Comments from senior program managers have indicated that they are aware of the differences in opinion regarding control and centralization, though they anticipate the CIO Model remedying this once it is completely implemented. Interviews with senior program management suggested a few other potential benefits of the CIO Model, such as:

- a decrease in the duplication of IM/IT assets due to holistic IM/IT solutions;
- a decrease in overall IM/IT departmental spending due to coordinated and controlled IM/IT expenditures; and
- an increase in awareness of stakeholder IM/IT activities due to improved oversight of IM/IT requirements and IT projects.

In short, according to program documentation and senior program managers, the implementation of the CIO Model will enable the Defence IM/IT Programme to more effectively govern Defence IM/IT in DND/CAF.

Implementation Status

The implementation of the CIO Model has been underway since March 2015; however, there is an unclear consensus as to its current status.[29] Interviews with program managers suggest that there are some aspects that have been implemented, allowing for improved oversight of IT projects and expenditures internal to ADM(IM). However, FPG 18/19 states that the implementation of the Defence CIO Model was to be

[28] Defence CIO Model – DM Briefing February 12, 2018.
[29] Ibid.

completed in the spring of 2017,[30] while FPG 19/20 states that one of the key activities would be to implement the Defence CIO Model.[31] Likewise, interviews with senior program managers and other stakeholders indicated a range of knowledge regarding the implementation status of the CIO Model; from currently implemented, implementation in progress, to not yet implemented. Further, some stakeholders were completely unaware of the CIO Model's existence. For this reason, it is difficult to ascertain the extent to which the governance model has been implemented and its subsequent impact on program effectiveness.

Roles and Responsibilities

Although the DAODs 6000[32] series have named ADM(IM) as the functional authority over Defence IM/IT, confusion among service providers regarding ARAs persists.[33] Interviews and comments from the questionnaire from service providers have indicated that this is a result of ARAs not being clearly delineated. Thus, it is difficult to determine who is responsible for components of Defence IM/IT among not only service providers internal to DND/CAF, but also with SSC. This is supported by the Gartner Consulting report, which found "a high incidence of uncoordinated and overlapping service delivery due to confusion about roles and responsibilities."[34] Conversely, senior program managers state that ARA delineation is currently satisfactory; however it needs to be communicated better to L1s. Nevertheless, the lack of clearly defined roles has led to a lack of coordination with IM/IT service providers due to the uncertainty of IT asset ownership, which has negatively impacted the effectiveness of the program.

Key Finding 7: Numerous policies and related documentation remain in draft format, making it difficult for service providers to ascertain the approval status of policies. This is further challenged by an inability for enforcement and inconsistent dissemination of policies and related documentation.

The extensive number of policies, guidance, directives and other related documentation presents a challenge for the Defence IM/IT Programme's governance. The evaluation noted a considerable number of documents that were identified as important.[35] Comments from the service provider questionnaire expressed confusion with the number of policies that currently exist as well as the redundancies and contradictions believed to exist between them. Upon examination of Defence IM/IT Programme policy

[30] Defence IM/IT Functional Planning Guidance 2018-19.
[31] Defence IM/IT Functional Planning Guidance 2019-20.
[32] DAOD 6000 Information Management and Information Technology.
[33] DND and CAF IM and IT Policy Framework.
[34] Defence IM/IT Programme: Executive Summary, Gartner Consulting (2015).
[35] Documents on the ADM(IM) Defence Intranet website,or on the Defence IM/IT Programme Sharepoint website as "Key Documents." The Defence Intranet website refers to seven such documents, while the Sharepoint website refers to nineteen different folders and nine different other files, as well as five DAODs associated with Defence IM/IT. The Defence Intranet additionally refers to DAOD 6420, 6421, 6423 but lead to inactive webpages.

documentation, a particular case highlighted this issue; the DND and CAF IM and IT Policy Framework referred to a DAOD 6004; however it could not be found after further research.[36]

The issue of numerous policy documents is amplified due to the number of documents that remain in draft format, which contributes to confusion among stakeholder organizations. The evaluation found a number of governance documents that have remained in draft format despite being published, such as the IM/IT Governance Framework and the FPG 18/19. As a result, service providers are unaware when a particular document has been approved and come into effect. Thus, the Defence IM/IT Programme's initiatives may not be followed or undertaken by service providers because they are operating with the assumption that they are not yet in force.

Enforcement of policies is another challenge that the Defence IM/IT Programme faces. There is no mechanism to ensure that stakeholders align themselves with the Defence IM/IT Programme's strategies. Interviews with senior program management indicated that this is a known issue within the organization and have noted that they do not have the capacity to force compliance or have appropriate repercussions for those who do not comply with initiatives that are outlined in the FPG. The service provider questionnaire found that 93 percent of respondents take the Defence IM/IT Programme's FPG into consideration. However, interviewees expressed that while the FPG may be taken into consideration, their own organizational IM/IT requirements will take precedence over those of the Defence IM/IT Programme. Interviews with senior program officials suggest that they believe the CIO Model should resolve this issue. Both senior program officials and service providers acknowledge that once the CIO Model comes into full effect, stakeholders will have no other option but to comply with the Defence IM/IT Programme's requirements in order to ensure that their own organizational needs are fulfilled. However, as the implementation of the CIO Model is presumed to be incomplete, this cannot yet be confirmed.

In conjunction with the numerous policies that are released by the Defence IM/IT Programme, incoherent dissemination is a source of confusion for service providers. A particular example was demonstrated by the Defence IM/IT Programme's FPG. The FPG is necessary to help guide organizations as they develop their annual IM/IT business plans; however its means of dissemination is largely unknown by both ADM(IM) and other key stakeholders. Comments from the service provider questionnaire and interviews have indicated that the FPG is often released too late, or that they were left unaware when it was published.[37] The FPG is not the sole instance of this issue, which results in a lack of awareness of a number of strategic documents and organizational changes within the Defence IM/IT Programme. The promulgation of policies is not

[36] DND and CAF IM and IT Policy Framework.

[37] When FPG 19/20 was released there was a link provided in one of the Defence Team Updates in May 2018. However, key organizational IM/IT liaisons remained unaware of its release when asked during interviews.

widely understood or coordinated by the Defence IM/IT Programme. As discussed under Key Finding 5, the Defence IM/IT Programme does not have an effective communication strategy.

ADM(RS) Recommendation

2. To strengthen governance and oversight of the Defence IM/IT Programme, ADM(IM) should:

   a. Establish and formalize Defence IM/IT ARAs.

   b. Review and consolidate Defence IM/IT policies to ensure alignment with established ARAs.

   c. Establish a communication strategy to ensure that ARAs, policies, guidance and directives are disseminated holistically to stakeholders in DND/CAF.

OPI: VCDS, ADM(IM)

Key Finding 8: Improvements are currently underway to enhance processes as the Defence IM/IT Programme finds it challenging to keep up with and incorporate evolving technologies in its delivery of systems, products and services.

The evaluation identified multiple challenge areas within IT processes, namely: timeliness, the Defence IM/IT Programme's ability to deliver IT requirements within a reasonable time; interoperability, the Defence IM/IT Programme's ability to deliver IT requirements that work within the existing networks of DND/CAF; and resources, the Defence IM/IT Programme's capacity to deliver IT requirements. These issue areas were noted through interviews, program documentation, as well as responses from the service provider questionnaire.

The Defence IM/IT Programme, and in particular DGIMPD, have undertaken a number of initiatives to improve the agility of IT projects delivered. Phase 1 of the Project Approval Process Renewal is underway and should improve the timelines of the major capital procurement process. This is discussed further in Key Finding 13. DGIMPD is also exploring means to break down larger projects that go through the major capital procurement process into smaller minor capital project components which the IM group can deliver more quickly. When interviewed, program management stated that 53 minor projects have advanced and ten have been completed. Further, the Defence IM/IT Programme has adopted a continuous intake process, which will allow "urgent/time sensitive" requirements to be approved more quickly as opposed to waiting for the general approval process of the Defence IM/IT Programme.[38]

[38] Defence IM/IT Programme Update to Stakeholders, (2018).

The Defence IM/IT Programme has improved its oversight of IT projects, which may contribute to improved interoperability. In this regard, DGIMPD hopes to have a greater capacity to intervene as IT projects and IT requirements are designed to ensure their interoperability before they have been delivered. Such interventions have the ability to ensure that IT deliverables account for the rapid pace of technological advancement and remain up-to-date. Interviews with senior management have indicated that the Defence IM/IT Programme is working to break down silos within the program to prevent the development of IT projects in isolation. In doing so, there will be a greater awareness of projects underway to ensure that they are able to connect with each other. The evaluation also noted that the Chief Security and Technology Architect,[39] which was newly established by Director General Enterprise Application Services (DGEAS) in 2018, will also work to improve interoperability and network integration, as is discussed in Key Finding 13.

Addressing the issue of resources, DGIMPD is exploring means to overcome this challenge. For some projects, DGIMPD has used Vote 1 funding, which is released earlier than Vote 5 funding, so that project managers can be involved earlier in an IT project's development. This is likewise discussed in Key Finding 4. Additionally, DGIMPD has adopted a training program called the Engineering Officer Development Program[40] with the intent to bridge two engineering graduate students per fiscal year. In doing so, they hope to meet the increasing personnel demands required by the increasing number of IT projects required by DND/CAF.

Key Finding 9: IT support provided by service management centres is inconsistent across DND/CAF, despite the establishment of SLAs by the Defence IM/IT Programme.

The evaluation noted challenges facing Service Management Centres (SMC) following the consolidation of IT help desks across DND/CAF, as per the Defence Renewal.[41] Fifty-six percent of respondents to the service provider questionnaire disagree/strongly disagree with the statement: "The Defence IM/IT Programme governance strategy is effective in providing end-user support service and maintenance." Comments from interviews with program managers have indicated that there are insufficient personnel resources given to SMCs to effectively provide IT support services. Interviews with

> *"The ITSM SMC Framework is a great concept and has tremendous potential to streamline and achieve standardized/predictable levels of service. To achieve its full potential, consideration should be given to the O&E [organization and establishments] of the SMCs."*

[39] There is still discussion regarding the name. It may be adjusted to Chief Security and Technology Architect for Information Systems.
[40] DGIMPD, Program Assessment FY 18/19-FY 20/21.
[41] Defence Renewal Initiative 3.1 – IT Service Management.

senior program managers have indicated that this is related to the transfer of FTEs to SSC, as discussed in Key Finding 11. Further, questionnaire comments have identified challenges arising from SMCs not understanding the clients' needs. Interviews with senior program managers have revealed that the transition to regional SMCs has resulted in service providers from one environment now having to take on IT support responsibilities for others outside of their own operational environment but under their regional authority. As a result, they may not have the appropriate understanding of IT support needs for those outside of their operational environment.

An additional concern raised was the variance of IT support levels across DND/CAF. The Enterprise IT Service Agreement (ESA) was created as part of the ITSM Project, which established SLAs between L1 IT service providers and DND/CAF. However, despite the establishment of SLAs, comments from the service provider questionnaire suggest that there are disparities of IT support. In particular, they noted a difference in IT support inside and outside the National Capital Region (NCR). Upon further examination, from April 1, 2015 to October 1, 2018, incident reports were closed within SLA targets between a range of 62 percent at the Greenwood SMC and 90 percent at the National Cadet Junior and Canadian Ranger Support Group SMC. It was noted, however, that SMCs farther from the NCR had lower percentages (below 80 percent), while SMCs that were closer to the NCR had higher percentages (above 80 percent), which supports comments on disparity.[42] Despite the creation of the ESA, which outlines standards, these challenges remain. This may be an indication of a lack of uniform policy enforcement or a lack of understanding of ARAs, which is highlighted in Key Findings 6 and 7.

ADM(RS) Recommendation

See recommendation 2
OPI: VCDS, ADM(IM)

2.2.3 Impact of the Transfer of Services to SSC

Key Finding 10: Delays in IT services provided by SSC have resulted in ineffective and slow support to operations.

An analysis of the written comments obtained from the questionnaire and interviews with various stakeholders showed that SSC's response time to incidents has been slow; 88 percent of respondents were either very unsatisfied or unsatisfied about service response time from SSC. Comments to the questionnaire also revealed that SSC did not have the appropriate resources and staffing required to provide timely, effective or affordable IM/IT support. Administrative data obtained from the data entry tool

[42] ITSM ASSYST-Data obtained from the Administrative data tool ASSYST. Retrieved on September 26, 2018.

ASSYST[43] supported these concerns. Based on the ASSYST data, approximately 25 percent of SSC incidents[44] remained open for more than 180 days.

In response to the questionnaire, 82 percent of those queried are either very unsatisfied or unsatisfied with SSC IT projects and services being delivered on budget. Similarly, during key stakeholder interviews, a representative from the Environmental Commands mentioned that of the 89 requirements they had requested in 2016, SSC delivered on only three or four, making it very difficult for future planning.

Key Finding 11: Until the SLA between DND/CAF and SSC is signed, the monitoring of service quality and standards will be difficult.

Service Standards

Another cause of concern among IT stakeholders resulting in confusion and delays was the lack of a signed SLA between the two departments. This means that currently there is no clear delineation of the required or expected service level expectations (i.e. service standards are still pending).

According to the draft SLA document, SSC will be developing corporate wide service standards and associated operational performance targets for all of its services. In the interim, service targets are being met through service level expectations within the Service Catalogue, of which most are undefined.[45]The Evaluation of Distributed Services (SSC, 2016)[46] covered the issue of lack of an SLA and standards. The evaluation underlined that “interviewees from large government departments underscored that well-documented processes with clear service standards and service time, which reflect new services, policy requirements and new systems in place were fundamental to ensuring the functionality of end-user workstations.”[47]

[43] Data obtained from the Administrative data tool ASSYST. Retrieved on September 26, 2018. ASSYST is an application that provides a consolidated approach for IT service management and IT infrastructure library. ASSYST is now commonly used by all service providers across the DND/CAF and replaces legacy systems formerly used by individual service providers. Source: Canada. Department of National Defence. DIMEI 7: ASSYST Enterprise. Online: 2016. http://dsblcsf.ottawa-hull.mil.ca/apps/details.asp?App=ASSYST&ShowAllDocs=1&. Accessed: July 27, 2016.

[44] Unplanned interruption of services. (Source: Evaluation of Information Systems Lifecycle).

[45] Audit of Shared Services Canada’s Information Technology Asset Management, SSC June 2017. Last consulted on September 7, 2018. https://www.canada.ca/en/shared-services/corporate/publications/audit-shared-services-canada-information-technology-asset-management.html.

[46] Evaluation of Distributed Services, SSC (2016). https://www.canada.ca/en/shared-services/corporate/publications/evaluation-distributed-computing-services.html#a11. Last retrieved December 5, 2018.

[47] Ibid.

Roles and Responsibilities

Not having an approved SLA with clear delineation of roles and responsibilities between the Defence IM/IT Programme and SSC has continued to be problematic. This issue was also noted in the previous evaluation of the Information Systems Lifecycle Program. The questionnaire responses indicated that only 24 percent of stakeholders agreed that roles and responsibilities were clearly defined (76 percent either strongly disagreed or disagreed). They noted that multiple service providers did not have defined service level expectations and had unclear lines of responsibility with SSC. For example, the intelligence systems exist in all three Environmental Commands. Some of the unclassified intelligence systems have limited support due to SSC discontinuing upgrades because it is not clear who is responsible for these services. Another example was that, although SSC was to be responsible for BlackBerry support according to the Order-in-Council, a significant portion of this support has been handed back to DND service desks.

The Audit of IT Asset Management (SSC, 2017)[48] outlined the communication problems with clients of SSC in regards to roles and responsibilities and mainly linked it to the "absence of a signed materiel management framework for inventory and disposal management." In the absence of any service agreement, DND's end-users believed that SSC did not have a clear understanding of defence requirements and/or comply with service standards which led to putting clients at great risk on a number of fronts, including security.

The evaluation also examined the effect on operational requirements resulting from the transfer of services to SSC. Comments obtained from interviews and the questionnaire underlined that SSC did not have any deliberate processes to address urgent operational requirements due to a lack of clear roles and responsibilities between the two departments. In this regard, the questionnaire respondents provided examples of situations that affected operations negatively, such as the email server that went down during a domestic operation. The domestic operation happened during a weekend and at the time, SSC did not have staff "on call" to provide/recover services. In another instance, the Navy provided an example concerning equipment that optimized the bandwidth on ships for services such as the Defence Wide Area Network. SSC put a policy in place requiring the removal of this equipment resulting in a 30 percent decrease in bandwidth and operating environment. Further, it was commented that SSC did not have any obligation to restore the loss of bandwidth. The evaluation also heard through the questionnaire responses that SSC has no personnel in the European Union to service DND/CAF personnel. In other cases, it was mentioned that urgent operational

[48] Audit of Shared Services Canada's Information Technology Asset Management, SSC June 2017. Last consulted on September 7, 2018. https://www.canada.ca/en/shared-services/corporate/publications/audit-shared-services-canada-information-technology-asset-management.html.

requirements have only been successfully addressed when communication bridges were established (i.e. based on personal relationships).

The evaluation received numerous additional comments of the impact of services delivered by SSC impacting the functioning of Canadian Forces Bases. This is outside this evaluation's scope but is discussed in the Evaluation of CAF Bases and Wings Sustainment Programs.

DND/CAF end-users believe that similar problems may persist unless a draft SLA is signed and distributed, setting clear standards and delineation of roles and responsibilities. SSC is currently undertaking a number of initiatives to improve service quality to the departments it serves.

ADM(RS) Observation

Once the SSC client-facing services initiative is fully implemented, establishing and monitoring service standards in collaboration with SSC would be advantageous for future performance reviews and establishing a baseline.

2.3 Performance—Demonstration of Economy and Efficiency

2.3.1 Demonstration of Economy

Key Finding 12: This evaluation is currently unable to determine the actual cost of the program. Expenditures tracking remains a challenge, and the Defence IM/IT Programme has limited visibility for at least half of Departmental IT expenditures.

Costing

Data analysis revealed a challenge in determining an accurate total cost of Defence IT activities. During this evaluation, the Defence IT expenditures were examined from multiple lenses using costs assigned to: the Program Alignment Architecture (PAA) elements; the DRF Restated Expenditures Report; and the IT Expenditure Report submitted to TBS. The costs derived from each of those lenses shall be discussed in the following sections.

PAA Elements

The first approach was to determine the cost of the program from the legacy PAA elements, as expenditures are still being recorded in this manner. Under the PAA system of attributions, most IT expenditures were to be within the sub-program 4.4: Information Systems Lifecycle (4.4.1-4.4.4). During this evaluation, it was found that

5.1.1 was also a PAA sub-sub-program with IT-related expenditures. Those five PAA elements within DRMIS totalled $1.1 billion in FY 2017/18.

It is important to note that the relationship between PAA elements and DRF programs is not one-to-one, but rather multi-dimensional. Specifically with regard to IT expenditures, the seven DRF programs[49] included in the Defence IM/IT Programme are mapped from 13 PAA elements.[50] However, those 13 PAA elements are mapped to 22 DRF programs,[51] of which 15 are not considered part of the Defence IM/IT Programme.[52] The 13 PAA elements total $5 billion in FY 2017/18. This makes it challenging to quantify a definite cost of the Defence IM/IT Programme.

Both systems of expenditure attribution have been criticized, and there are difficulties when comparing the legacy PAA system of expenditure attribution to that of a relatively new and not fully implemented DRF system. Although both systems of attributions were recorded in DRMIS, the systems are not equal in application, and there will be some similarities and some divergences between the two.

DRF Restated Expenditures Report

A mapping exercise produced a crosswalk between PAA elements and DRF programs, and has presumably made the most appropriate correlations between the two systems and their relative elements. The restated expenditures for IT activities was $795,907,000 for FY 2017/18. Program managers noted that the move towards L1 silos has prevented the Defence IM/IT Programme from capturing the total IT spending under the DRF.

The shift from PAAs to the current DRF program expenditures was required of all departments by the 2016 TB Policy on Results. The PAA was mapped to the DRF programs, and as of April 1, 2018, the “tracking and reporting of financial, human resources and program results by the DRF” was reported to be in place.[53] However, at the time of this evaluation, DRF attribution rules for DRMIS had yet to be implemented, which could further deteriorate the accuracy and consistency of expenditure reporting.

[49] IT DRF programs: 1.5, 2.6, 4.6, 5.4, 6.5, 7.6, 7.7.

[50] IT PAA elements: 1.1.3, 3.1.5, 3.2.5, 3.2.6, 3.3.5, 3.4.5, 4.2.5, 4.4.1, 4.4.2, 4.4.3, 4.4.4, 5.1.1, 5.1.2.

[51] DRF programs related to IT PAAs: 1.2, 1.5, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 3.8, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 5.4, 6.5, 7.6, 7.7.

[52] PAA to DRF Crosswalk.

[53] DRF, Brief to the Comptroller’s Training and Development Forum, November 9-10, 2017, ppt. Accessed October 22, 2018, http://cfo-dpf.mil.ca/assets/FinCS_Intranet/docs/en/learning-careers/ndctdf-drf-1-2017-2018.ppt.

IT Expenditure Report

The IT expenditure report submitted to TBS appears to be the most consistent means of capturing IT expenditures and trends, as well as the only viable comparison available with other government departments (OGD), although possibly not comprehensive for determining the cost of the Defence IM/IT Programme in its entirety. The IT expenditure report considers IT expenditures from across all seven DRF Core Responsibilities, and portions are submitted by individual L1s to the Defence IM/IT Programme for consolidation. While figures are taken from DRMIS, the official financial tool of record for DND/CAF, some calculations may be performed post-extraction, according to senior program managers. Program management noted that this figure is the true statement of IT spending in the department and is certified by all L1s, the CIO, and the CFO, and is likely the most consistent for trending purposes.

As the IT expenditure report is standardized across the federal government, it is the only source to illustrate that the reported DND IT expenditures are stable compared to other similar government departments on a number of points, which are illustrated in Figures 1 and 2: IT Expenditures per FTE and IT Expenditures/Departmental Expenditures.

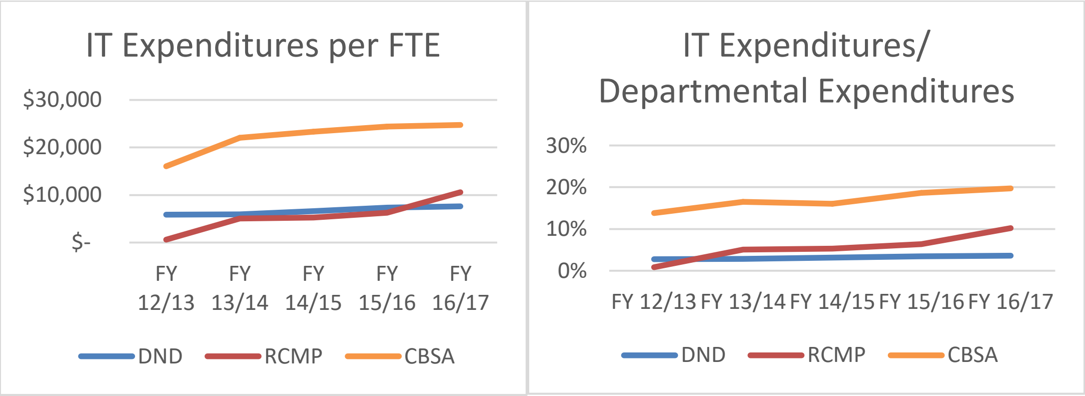


Figure 1 and Figure 2. IT Expenditures per FTE and IT Expenditures/Departmental Expenditures. Source: TBS IT Expenditure Reports (net of exclusions) from DND, Royal Canadian Mounted Police (RCMP), Canada Border Services Agency (CBSA); Defence Performance Report Human Resource and financial data for DND, RCMP, CBSA.

Notably, the IT Expenditure Report submitted to TBS from each department has specific exclusions, historically stated as being in the 20-25 percent range of all IT expenditures for DND/CAF. During interviews, it was articulated by senior management that the Defence IT program spends in the neighbourhood of $1 billion per annum; this is accurate if referring to the IT expenditures reported to TBS plus the exclusions.

Given the discrepancies between the three sets of data, this evaluation could not reconcile the total cost of the Defence IM/IT Programme definitively.

Expenditure Tracking

Under the PAA there were challenges, which were articulated in the Evaluation of the Information Systems Lifecycle Program (2016). Within that report, Key Finding 17 stated: "The department has not accurately tracked expenditures related to the IS Lifecycle Program. As such, it was difficult to determine the extent to which the department has used cost-effective means in the production of outputs." That finding, along with another, resulted in the following recommendation: "There is a need to improve tracking of program expenditures, particularly at the output level (i.e. project management costs, user support costs, in-service support costs)."[54] As the evidence in the previous section suggests, the trending difficulties have continued. Interviewees also suggested that other L1s may not have the same level of accountability or rigorous reporting under the current governance model compared to the ADM(IM), thus weakening the precision of expenditures being attributed to the DRMIS figures.

The DND/CAF CIO has had limited visibility and control over 50-57 percent of IT expenditures. Over three fiscal years, an average of 45 percent of the expenditures attributed to the five IT PAA elements were made by ADM(IM), as can be seen in Figure 3: DND/CAF IT Spending Visibility. This is corroborated by interview evidence, where Defence IM/IT Programme stakeholders referenced the inability to determine how other L1s are spending their portion of the program money.

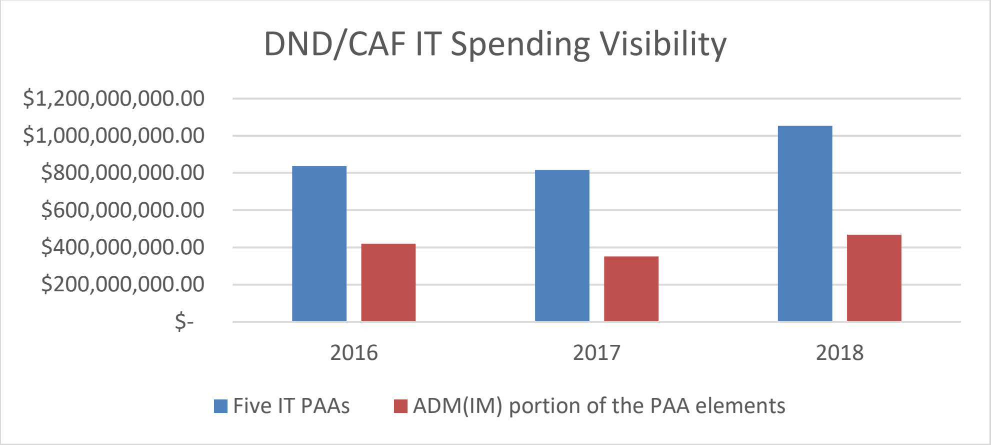


Figure 3. DND/CAF IT Spending Visibility. Source: DRMIS.

A performance measurement strategy combined with improved expenditure tracking could alleviate the observed issues. As part of the implementation of the DRF, Program Inventory Profiles are designed to enable the collection of data through performance measurement indicators in order to support monitoring, decision making, and evaluations of departmental programs. Portions of the performance framework should ideally link expenditures to program outputs and activities. "The indicators currently in

[54] Evaluation of the Info Systems Lifecycle Program, V 2.2.

the DRF will require attention in order to improve the depth, breadth and validity of our performance measurement, for both external reporting and internal program management."[55] As part of the priorities for FY 2018/19 for management improvements relating to corporate performance measurement, a working group has been established to focus on the "IT financial integration of the DRF into DND systems."[56] This initiative aligns with the evaluation's following recommendation.

ADM(RS) Recommendation

3. As part of the implementation of the revised governance model, ensure accurate attribution and tracking of expenditures throughout the Defence IM/IT programme with links to the performance framework.
OPI: ADM(IM)
OCI: ADM(Fin), C Prog

2.3.2 Demonstration of Efficiency

Key Finding 13: There exists a duplication of systems, networks and efforts. The creation of Chief Technology and Security Architect for Information Systems (CTSAIS) and the Chief Application Architect aim to reduce these and enhance system integration.

The current practices in the Defence IM/IT Programme lend to a multitude of inefficiencies, and inter-organizational integration is insufficient. Capabilities are being delivered in isolation with no adequate system integration process, and the proportion of IT applications and networks that are not fully amalgamated within the IT architecture remains unknown. DGEAS within ADM(IM) is responsible for 173 applications, which is between 3 and 9 percent of the total amount of IT applications within DND, many with the same data but lacking interoperability.[57] Other L1s create their own IT solutions for various reasons, most without integration interfaces. Even if duplications are identified and communicated, interviewees have stated that it is often more convenient to continue as is than to make the necessary changes within the total architecture. The situation is best described in the Defence IM/IT Programme Application Strategy, 2017:

"We need to coordinate better – a lot of duplication of effort that leads to resources being used inefficiently."

[55] Corporate Performance Measurement Improvement Plan 2018-19.
[56] Corporate Performance Measurement Improvement Plan 2018-19, Chief of Programme, Vice Chief of the Defence Staff, 2018-06-19, Final Draft.
[57] Close-out Report notes that National Defence has over 5000 applications.

> "The distributed nature of DND/CAF application delivery has resulted in a portfolio where some capabilities are enabled by multiple applications. Consequently, it is not uncommon to discover different Defence organizations using different applications to perform the same functions. Not only is the duplication of functionality costly to build and maintain it also poses significant challenges to the delivery of integrated and interoperable Defence capabilities."

In order to be better aligned with industry and technology trends, DND/CAF IT solutions need to move from the legacy integration process to a modernized design, which will also simplify application portfolio integration enabled during the design phase.[58] In line with this direction, the Defence Renewal Initiative 3.2 – Applications Portfolio Management, which has already realized a reinvestment opportunity of $13.4 million, aimed to "ascertain misalignments between the application portfolio and business requirements, allowing managers and other IT professionals to adjust their resources accordingly." This initiative has already retired or removed duplicates of 1,922 applications, and improved the "overall stewardship and maturity of application management practices across DND/CAF." [59]

Further to the previous improvements, the Innovation Systems Engineering and Architecture Coordination Programme supports the CTSAIS[60] within Director Information Management Engineering and Integration (DIMEI) in their role to "develop and oversee the implementation of technical and security standards for all architecture, engineering, configuration and integration of IT and CIS [Communication and Information System] that support corporate, C2 [Command and Control], and ISR [Intelligence, Surveillance and Reconnaissance] systems in the DND/CAF."[61] In 2018, DGEAS was established as the Chief Application Architect as mentioned in Key Finding 8. These roles and their related processes should further reduce duplications and the associated costs. Additionally, these roles should have a positive impact on SSE initiative 68 - Integrate existing and future assets into a networked, joint system-of-systems that will enable the flow of information among multiple, interconnected platforms and operational headquarters. One example given was standardizing anti-virus software from various versions to one tool, aiding overall efficiency. It was noted that in order for the CTSAIS role to be most effective, the impact and exact purpose of the position should be properly communicated to stakeholders both internally and externally to the Defence IM/IT Programme, as well as ensure that official documents have the appropriate levels of authority.

[58] Defence IM/IT Programme Application Strategy, 2017.

[59] Defence Renewal Team Close-out Report noted that National Defence has over 5000 applications. Program Senior Managers advised that no more than 1950 applications currently (2019) exist.

[60] The Information Systems Design Authority, including the architects, will fulfill this role.

[61] Source: https://collaboration-img.forces.mil.ca/sites/DIMEI/D5/Pages/D5Home.aspx, accessed December 11, 2018.

Key Finding 14: There are enhancements currently being implemented to improve project management and delivery.

The new direction of project management and delivery within the Defence IM/IT Programme is aiming to become more agile and time conscious in order to keep pace with ever-evolving technology. Projects are currently taking years in approvals and longer in implementation, leading to solutions being delivered that no longer fit within advancing technologies. The evaluation heard from several interviewees and questionnaire responses that project management processes have been criticized for these reasons, and solutions are being implemented to compensate for any limitations in the current methods.

> *"The complex processes associated with the capital projects and procurement are very slow and cumbersome, the process cannot keep up with the rate of change of technology."*

The Project Approval Directive (PAD) (2015) makes a similar observation: "Due to historical problems related to cost and schedule overruns, IT enabled projects are subject to additional oversight at a Government of Canada level."[62] Of the 13 projects with definition phase dates available, 69 percent of those projects were late entering the definition phase, with a total average variance of those late projects of 15 months.[63] Analysis of the service provider questionnaire disseminated by this evaluation indicates frustration concerning certain aspects of IT project delivery. Of those who responded, 65 percent were either very unsatisfied or unsatisfied with IT projects/requirements being delivered on time. Budget concerns were more neutral, with 47 percent expressing levels of dissatisfaction and 53 percent voicing levels of satisfaction. IT projects seem to be delivered in alignment with technical and operational requirements, with 77 percent of respondents communicating satisfaction in this area.

Project reporting methods are receiving enhancements to aid in overall efficiency for both project managers and decision makers. The Capability Investment Database (CID) is the existing storage location for all project information and documentation and is being replaced by a new system. As of April 1, 2018, no new projects have been entered in the CID as it is being decommissioned. In the interim, DRMIS will be used as a repository, in conjunction with GCDOCS for working files. Interview evidence suggests this has unfortunately led to temporary confusion, inaccuracies and duplication of efforts, as project information for current initiatives has to be updated in multiple systems in addition to varying stakeholder requested reports. Currently, there are 22 reports produced containing similar project information but for different stakeholders. These issues should be addressed by the new approach, DRMIS Project System (PS) Module,

[62] Source: PAD, 2015, An.B.1.2.
[63] IMPD Portfolio Brief, July 2018.

which is anticipated to be in full operational capacity by March 31, 2020. The DRMIS PS Module will be the single system for "enterprise-wide reporting and analysis, supporting strategic day-to-day management of the Defence Services Programme." [64]

In the IT domain, it is commonly understood that original IT requirements change because the nature of IT changes rapidly with time. Most IT projects deliver capabilities that are technologically out of date upon completion. Project agility is seen as crucial in order to be more responsive to the changing dynamics of IT. One service provider, for example, would like to have the ability to develop and test small requirements quickly in order to facilitate making rapid changes. DGIMPD expressed a similar sentiment when he discussed wanting to be able to "fail early" thereby facilitating changes in order to meet requirements.

Project measurement is another area where improvements are being employed. C Prog is trying to develop a standard way of monitoring all projects in the wake of SSE, and aligning different project measuring strategies to ensure consistency. The funding model is also being examined, as the process to incorporate project management staff earlier in the process is recognized as pertinent. Although Vote 5 funding is not received until later in the project, Vote 5 staff can be funded by Vote 1 money, and Vote 1 funds are being allocated for non-accrual projects. These changes will modernize the process and better support project delivery.

SSE initiative 94 concerns improving defence procurement and aims to "reduce project development and approval time in the Department of National Defence by at least 50 percent for low-risk and low-complexity projects through improved internal coordination, increased delegation, and strengthened approval processes."[65] This is a continuation of the Project Approval Process Renewal, initiated in April 2012, which had the same goal for project timeline reduction while "ensuring the processes are both Treasury Board compliant, and supported by an effective risk management framework."[66] The redesigned process, originally intended to be in full operational capacity by FY 2016/17, is approved and underway for Phase 1. The 2015 PAD itself is also being updated, and training for users is being developed. This evaluation believes that the updated PAD and associated processes will improve overall efficiency.

Finding 15: Until a complete costing model between DND and SSC is signed, this evaluation is unable to identify any savings in the Defence IM/IT Programme expenses resulting from the transfer of services to SSC, and cannot accurately presume future savings.

[64] Defence IM/IT Programme Update to Stakeholders.

[65] http://dgpaapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf, accessed October 30, 2018.

[66] Source: PAD, 2015.

The Audit of Demand and Relationship Management (SSC, 2017)[67] identified weaknesses with the costing aspect of the financial management process in SCC, in particular with the cost recovery process. According to the audit's findings, costing requirements are not defined in many areas and there is a lack of a centralized costing guide. This leads to inconsistent costing of business requirements and inconsistent decision making, such as when and how much to charge partners for services. In addition, service requests were received through multiple channels and there is no process in place to communicate updates on their status. Similarly, the 2015 Office of the Auditor General Audit[68] of SSC also noted that a lack of approved costing model was also a challenge for their department.

> *"SSC has not developed consistent processes to determine costs and to measure progress and savings…SSC did not account for partner costs as part of the transition to a shared services model. As a result, the overall financial savings to the government as a whole will remain largely unknown."*

Both questionnaire and interview evidence suggested that many organizations within DND/CAF were required to reimburse SSC for certain services for which they should not have been charged. The respondents underlined the complexities of SSC's billing system and urged that serious consideration be given to the rationale for paying annual fees to SSC for services, such as basic voice and data. Some respondents argued that despite receiving personnel and funding transfer following the Order-In-Council, SSC did not fulfill all of its responsibilities leading to many delays which resulted in negative business impacts. One common complaint is SSC billing for recurring charges that were not implemented in negotiation with partners. In some cases, partners are now paying for recurring charges with no funding plan. As a result, many SSC projects are moving forward with funding pressures. One program manager mentioned that departments are now bearing the brunt of on-going costings (e.g., one time cost for the delivery of the service, and then continual monthly charges after the project has been delivered).

The evaluation team noted that OGDs were experiencing similar issues. Both the Canada Revenue Agency (CRA) and CBSA claimed that they were overcharged for data processing jobs performed by SSC.[69]

The evaluation team attempted, but could not make definite conclusions on costs per service to DND/CAF before and after the transfer of IT services to SSC, as these costs

[67] Audit of Demand and Relationship Management. SSC, 2017. Last consulted on October 25, 2018. https://www.canada.ca/en/shared-services/corporate/publications/audit-demand-relationship-management.html.

[68] 2015 Fall Reports of the Auditor General of Canada. Information Technology Shared Services. Last consulted on October 24, 2018. http://www.oag-bvg.gc.ca/internet/English/parl_oag_201602_04_e_41061.html.

[69] CBC News, September 2018. https://www.cbc.ca/news/politics/shared-services-cra-cbsa-overbilling-data-processing-dispute-1.4838887 Last retrieved: December 5, 2018.

were only available in the IT Expenditure Reports (in aggregated forms) submitted to TBS annually. The following list describes the transfer of resources and expenditures paid by DND/CAF since the inscription of SSC.

- 2011/12: Initial DND transfer of $318 million and 761 positions (was noted in the 2015 Evaluation of Information Lifecycle report and various Departmental documents).
- 2012/13: TBS IT Expenditure Report noted that there were $7,708,038 in non-recovered expenditures incurred for activities that fall under the responsibility of SSC.
- 2014/15: TBS IT Expenditure Report noted: $16.3 million increase (in software) mainly related to software-related charges by SSC.
- 2016/17: TBS IT Expenditure Report stated: An increase of $17.4 million in external services was due to an increase in charges from SSC and the use of temporary help services.

The questionnaire respondents also underlined inefficiencies that have caused frustration among the end-users and service providers. These were mostly in regards to policies and processes used by SSC. Some examples are as follows:

- With an inability to carry over funding, it was difficult to synchronize funds with projects that are multi-year in nature.
- The current procurement process generally takes close to a year, affecting document retention.
- In comparison, SSC quotes have often been higher than those that can be found in industry, and an approximate additional 20 percent surcharge has also been added to charges by SSC.

Many questionnaire respondents indicated that lifecycle management of DND/CAF IT equipment was another significant cause of inefficiencies. SSC's Audit of Information Technology Asset Management (2017) also had a finding in this regard: "SSC did not have accurate and sufficient information to support the management of IT assets throughout their lifecycle" and recommended that "the information required to manage the lifecycle of information technology assets should be captured in a consistent and accurate manner."[70]

Responding to the questionnaire, DND service providers and end-users commented that if properly life cycled, there would be smaller incremental costs for DND/CAF's maintenance of IT equipment such as server space. They urged to have the proper level of oversight by the DND/CAF CIO to ensure that the Department received the level of support it should to enable the defence of Canada.

[70] Audit of Shared Services Canada's Information Technology Asset Management, 2017.

In the meantime, the GC has passed an omnibus budget bill C44 (April 2017) that includes a measure allowing government departments and agencies the option of not using SSC for some IT equipment and services. For example, the Bill allows departments to not only go outside of SSC, but also to use the same vendors that SSC has already established as contacts. In that regard, DND should investigate other options that SSC could provide.

In all, the evaluation did not have sufficient data to determine any efficiencies resulted from transfer of DND/CAF IT services to SSC.

Annex A—Management Action Plan

ADM(RS) Recommendation

1. Review the process and prioritization methodology for requirements used by the Defence IM/IT Programme Intake Process in collaboration with stakeholders to further clarify/promote transparency.

Management Action

Review of the IM/IT Programme requirements prioritization framework to include all components of the IM/IT Programme in collaboration with stakeholders to further clarify/promote transparency (e.g., in-service support, transformation, infrastructure, innovation, etc.) in order to increase Programme visibility and better explain linkages of the various components and associated dependencies. Programme stakeholders and Centre for Operational Research and Analysis to participate.

OPI: ADM(IM)
Target Date: Status update to IMB May 2020. Updated prioritization framework by May 2021.

ADM(RS) Recommendation

2. To strengthen governance and oversight of the Defence IM/IT Programme, ADM(IM) should:

   a. Establish and formalize Defence IM/IT ARAs.
   b. Review and consolidate Defence IM/IT policies to ensure alignment with established ARAs.
   c. Establish a communication strategy to ensure that ARAs, policies, guidance and directives are disseminated holistically to stakeholders in DND/CAF.

Management Action

a. ADM(IM) to review Defence IM/IT ARAs and continue to work with the Corporate Secretary (Corp Sec) to ensure that updates are reflected in drafts in preparation for publication.
b. Policy team to update the IM/IT policies to reflect any adjustments to the ARAs.
c. Develop a communications strategy for the Defence IM/IT (Information) Programme to improve communication of ARAs, policies, guidance, and directives across DND/CAF.

OPI: VCDS (a), ADM(IM) (b & c)
Target Date:
a. Defence Governance advised they cannot provide a deadline as ARAs are on hold.
Note: ADM(IM) should confer with Corp Sec to set a deadline, if possible.
b. Once Corp Sec has updated ARAs, the policy team will complete the update of IM/IT policies reflecting ARA changes within 12 months afterwards.

c. Regardless of the hold on ARAs, a communication strategy for policies, guidance and directives will be drafted by September 2019.

ADM(RS) Recommendation

3. As part of the implementation of the revised governance model, ensure accurate attribution and tracking of expenditures throughout the Defence IM/IT Programme with links to the performance framework.

Management Action

DDIMP to continue to work with C Prog, ADM(Fin), and other L1s to determine a reasonable method to track IM/IT expenditures within DND/CAF. Several initiatives are underway to address the issue including finalizing the governance framework, collaborating with C Prog on the performance measurement improvement plan and streamlining the way IT expenditures are tracked and reported.

OPI: ADM(IM)
OCI: ADM(Fin), C Prog
Target Date: Progress report to IMB by May 2020

Annex B—Evaluation Methodology and Limitations

1.0 Methodology

1.1 Overview of Data Collection Methods

The evaluation of the Defence IM/IT Programme gathered data from a number of sources in order to assess the program. The research methodology relied on both qualitative and quantitative research methods which, through data triangulation, ensured the validity of data collected for analysis. Based on evidence collected, the evaluation developed objective findings concerning the relevance and performance of the program.

Data collection methods used for the evaluation include:

- Literature and document review;
- Key informant interviews;
- Service provider questionnaire; and
- Program and financial data reviews.

1.2 Details on Data Collection Methods

1.2.1 Literature and Document Review

As part of the planning phase of the evaluation, a preliminary document review was conducted to develop a foundational understanding of the Defence IM/IT Programme and its components as well as determine the scope of the evaluation. This was expanded upon during the conduct phase of the evaluation, as other documents were examined to find data that would help in the assessment of the relevance and performance of the program. Documents included: government websites; government documents; program documents, including business plans and strategic policy; and government reports.

1.2.2 Key Informant Interviews

In the conduct of the evaluation, it was recognized that the perspectives of both policy drivers internal to ADM(IM) and service providers external to ADM(IM) were necessary in the assessment of program relevance and effectiveness. Internal to ADM(IM), interviews were conducted with: Director General Information Management Technology and Strategic Planning; DGIMPD; DGEAS; Director General Information Management Operations, Chief of Staff COS(IM)/J6; Director Defence Information Management Planning; Director Business Relationship Management; and DIMEI. External to ADM(IM), interviews were conducted with: Canadian Joint Operations Command, Special Operations Forces Command, CF Intelligence Command, and the Environmental Commands (Canadian Army (CA), Royal Canadian Navy (RCN), Royal Canadian Air Force

(RCAF)). Some interviewees were contacted afterwards for further clarification of comments or additional examples for the corroboration of evidence.

1.2.3 Questionnaire

To engage a broader number of stakeholders, the evaluation developed two questionnaires in English and French. One of the questionnaires had questions focused on the policy driver perspectives of ADM(IM), and the other questionnaire had questions focused on the service provider perspectives external to ADM(IM). The service provider questionnaire was distributed to: ADM(Mat); ADM (Science and Technology) (ADM(S&T)); Chief of Military Personnel; CF Intelligence Command; Judge Advocate General; Strategic Joint Staff; Special Operations Forces Command; and the Environmental Commands (CA, RCAF, RCN). IM/IT representatives of their respective organizations were contacted to find individuals within the organization who would be most appropriate to respond to the topics discussed in the questionnaire. These were often managers, but it was not always the case. Once identified, the questionnaire was provided to these individuals for their response.

Ultimately, data from the policy driver questionnaire had to be withdrawn, as there was a lack of a holistic response to accurately represent the perspectives of ADM(IM). The service provider questionnaire had a response rate of 57 percent out of 48 administered questionnaires; however the evaluation team received responses from all contacted organizations, which provided the evaluation with a greater holistic view of service provider responses. Questionnaire responses were corroborated against interview comments to ensure validity.

1.2.4 Program and financial data reviews

Financial program data was used to evaluate economy and efficiency of the program. The observed data included FY 2012/13 to FY 2017/18. The data was extracted using DRMIS, the Departmental Results Report, and TB IT Expenditure Reports.

2.0 Limitations

Table B-1 describes the limitations and mitigation strategies employed in the evaluation process of the Programme.

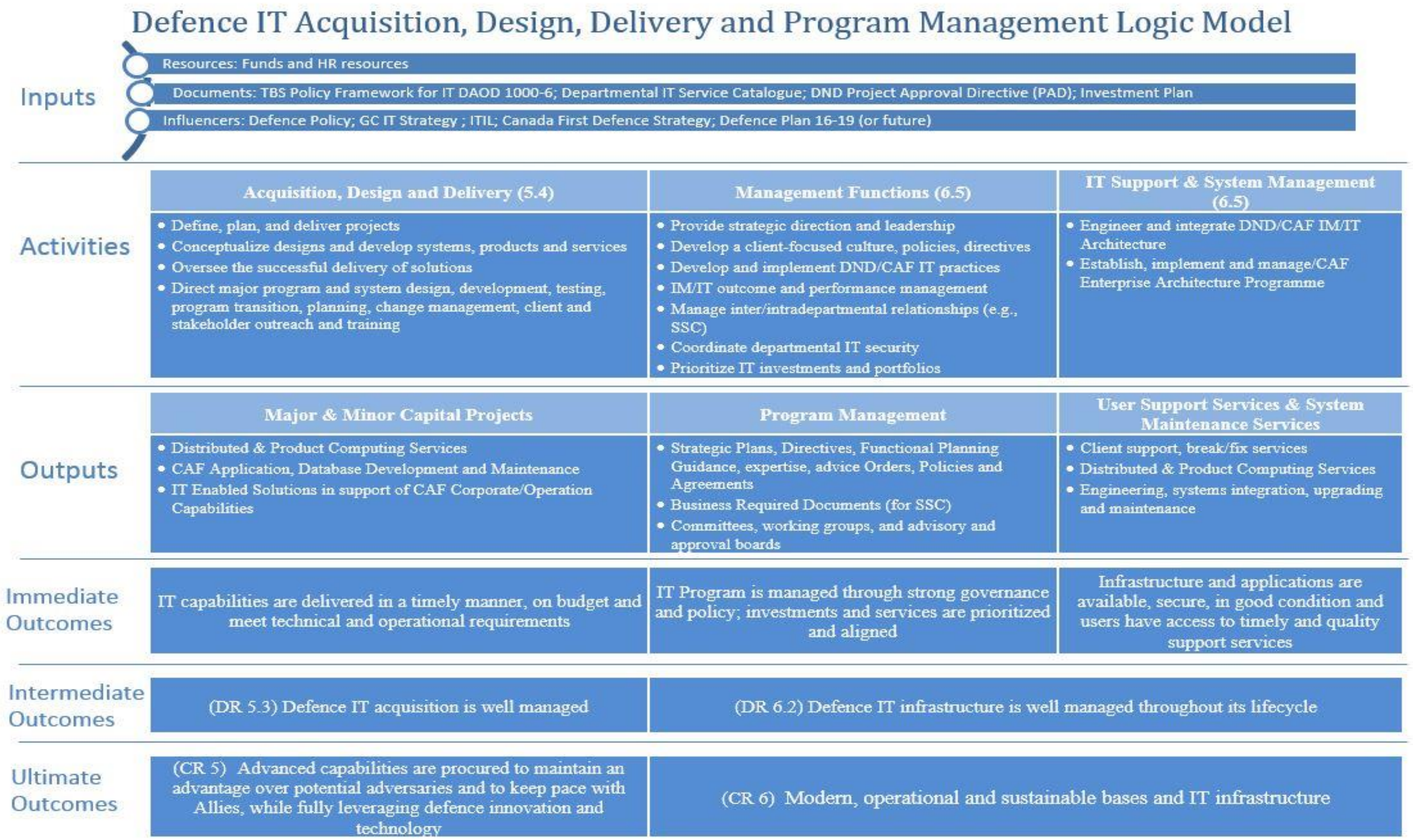
Limitation	Mitigation Strategy
Naming of the program: The Defence IM/IT Programme includes DRF programs 1.5, 2.6, 4.6, 5.4, 6.5, 7.6 and 7.7; for the purposes of this evaluation, 5.4 and 6.5 were to be examined. However, the evaluation team found it difficult to effectively analyse these two DRF programs in isolation of the broader	Taking into consideration these challenges, the evaluation team largely referred to the program as the Defence IM/IT Programme through the lens of DRF programs 5.4 and 6.5. Still, where necessary, the evaluation makes reference to the entire program when the entirety of Defence IM/IT is involved.

Defence IM/IT Programme. Namely, relevance, aspects of performance as well as economy, were key components of the evaluation that required a holistic look of the Defence IM/IT Programme. Removing these components from the context of the Defence IM/IT Programme would not provide an accurate analysis of these DRF programs for a number of reasons: • Firstly, the DRF programs are not understood in isolation of the Defence IM/IT Programme by most stakeholders. Thus, interviews and questionnaires given to stakeholders would not have been able to be successfully completed in the DRF program context. • Secondly, in regards to expenditures, the program itself requires a holistic view in order to more accurately determine and analyze its performance in this regard. • Thirdly, in certain instances, it is not logical to isolate the DRF programs from the context of the Defence IM/IT Programme. For example, program 6.5 is largely concerned with governance; however in order for it to be examined, its performance is determined in the context of governance over the Defence IM/IT Programme. Similar logic applies for relevance. • Lastly, the DRF programs are largely connected to each other in the makeup of the Defence IM/IT Programme. Only the cyber-related programs, which have recently come under the control of ADM(IM), are easily distinguishable from the Defence IM/IT Programme. Thus, examining them in isolation could not be done without looking at other issues in relation.	To prevent the unwarranted expansion of scope, the evaluation team made sure to stay within the confines of the three thematic issues of the evaluation: 1. whether the Defence IT requirements were aligned with future force capabilities; 2. the effectiveness of the governance model of the program; and 3. the impact of the transfer of services to SSC from an operational point of view.

Questionnaire responses: The evaluation team had difficulty receiving completed questionnaires from stakeholders. In particular, the team did not receive enough responses from some parts of ADM(IM), which would have resulted in a skewed perspective of the organization.	The team withdrew results collected from ADM(IM) and focused primarily on the questionnaire results from the service providers. Interview comments were relied upon to a greater extent for perspectives from ADM(IM) and corroborated with program data or other interviews for validity.
Questionnaire selection bias: Bias could arise based on the selection of the individuals or organizations chosen for the questionnaire, which could skew questionnaire results.	All service provider organizations were contacted for the purposes of the service provider questionnaire. Respondents were selected on the basis of experience with IM/IT topics and referred by their associates.
Interview bias: Bias could arise based on the subjective impressions and comments of interviewees, which could lead to biased views.	Interview comments were corroborated with other sources to ensure validity. Interview notes were conducted by more than one individual to confirm understanding of discussions and decrease the likelihood of bias.
Program Expenditure Validity: The evaluation team had difficulty ascertaining Programme expenditures as a result of conflicting financial data.	This is discussed further in the evaluation and was identified as an issue area within the program.

Table B-1. Evaluation Limitations and Mitigation Strategies. This table lists the limitations of the evaluation and the corresponding mitigation strategies.

Annex C—Logic Model



Defence IT Acquisition, Design, Delivery and Program Management Logic Model

Inputs	Resources: Funds and HR resources Documents: TBS Policy Framework for IT DAOD 1000-6; Departmental IT Service Catalogue; DND Project Approval Directive (PAD); Investment Plan Influencers: Defence Policy; GC IT Strategy ; ITIL; Canada First Defence Strategy; Defence Plan 16-19 (or future)		
Activities	**Acquisition, Design and Delivery (5.4)** • Define, plan, and deliver projects • Conceptualize designs and develop systems, products and services • Oversee the successful delivery of solutions • Direct major program and system design, development, testing, program transition, planning, change management, client and stakeholder outreach and training	**Management Functions (6.5)** • Provide strategic direction and leadership • Develop a client-focused culture, policies, directives • Develop and implement DND/CAF IT practices • IM/IT outcome and performance management • Manage inter/intradepartmental relationships (e.g., SSC) • Coordinate departmental IT security • Prioritize IT investments and portfolios	**IT Support & System Management (6.5)** • Engineer and integrate DND/CAF IM/IT Architecture • Establish, implement and manage/CAF Enterprise Architecture Programme
Outputs	**Major & Minor Capital Projects** • Distributed & Product Computing Services • CAF Application, Database Development and Maintenance • IT Enabled Solutions in support of CAF Corporate/Operation Capabilities	**Program Management** • Strategic Plans, Directives, Functional Planning Guidance, expertise, advice Orders, Policies and Agreements • Business Required Documents (for SSC) • Committees, working groups, and advisory and approval boards	**User Support Services & System Maintenance Services** • Client support, break/fix services • Distributed & Product Computing Services • Engineering, systems integration, upgrading and maintenance
Immediate Outcomes	IT capabilities are delivered in a timely manner, on budget and meet technical and operational requirements	IT Program is managed through strong governance and policy; investments and services are prioritized and aligned	Infrastructure and applications are available, secure, in good condition and users have access to timely and quality support services
Intermediate Outcomes	(DR 5.3) Defence IT acquisition is well managed	(DR 6.2) Defence IT infrastructure is well managed throughout its lifecycle	
Ultimate Outcomes	(CR 5) Advanced capabilities are procured to maintain an advantage over potential adversaries and to keep pace with Allies, while fully leveraging defence innovation and technology	(CR 6) Modern, operational and sustainable bases and IT infrastructure	

Figure C-1. Logic Model for the Defence IM/IT Programme This flowchart shows the relationship between the program's main activities, outputs and expected outcomes.

Annex D—Evaluation Matrix

Evaluation Matrix - Relevance					
Evaluation Issues/Questions	**Indicators**	**Program Administrative and Finance Data**	**Document & Literature Review**	**Key Informant Interviews**	**Questionnaire**
1.0 Is there a continuing need for the Defence IM/IT Programme?	1.1 The IT Acquisition, Services and Management Program provides necessary systems and services for DND/CAF operations.	No	Yes	Yes	No
	1.2 The program provides services and products that no other organization or program can deliver.	No	Yes	Yes	No
2.0 Are the objectives of the Defence IM/IT Programme consistent with the existing and emerging DND strategic objectives and federal government priorities?	2.1 Alignment between program activities, federal government priorities, and DND/CAF priorities.	No	Yes	No	No
3.0 Is the Defence IM/IT Programme consistent with the roles and responsibilities of the federal government and DND/CAF?	3.1 Alignment of the program with GC Acts and legislation.	No	Yes	No	No
	3.2 Alignment of the program with DND/CAF roles and responsibilities.	No	Yes	No	No

Table D-1. Evaluation Matrix—Relevance. This table indicates the data collection methods used to assess the evaluation issues/questions for determining the Defence IM/IT Programme's relevance.

Evaluation Matrix—Performance: Achievement of Expected Outcomes (Effectiveness)

Evaluation Issues/ Questions	Indicators	Program Administrative and Finance Data	Document & Literature Review	Key informant interviews	Questionnaire
4.1 Do IT system requirements align with the needs of future force capabilities?	4.1.1 Evidence that IT infrastructure, systems and application requirements align with the needs of future force capabilities.	No	Yes	Yes	No
	4.1.2 Evidence that IT deliverables align with the predicted future force capabilities.	No	Yes	Yes	No
	4.1.3 Evidence that IT deliverables align with the predicted future force capabilities.	No	Yes	Yes	No
4.2 To what extent does the Defence IM/IT Programme have the right governance strategy to achieve its objectives?	4.2.1 The IT program is managed through strong governance and policy; investments and services are prioritized and aligned.	No	Yes	Yes	Yes
	4.2.2 Impact of the governance strategy in enabling the IT program in delivering systems, products and services.	No	Yes	Yes	Yes
	4.2.3 Impact of the governance strategy in providing end-user support services and maintenance.	No	Yes	Yes	Yes
4.3 What is the impact of the transfer of services from the	4.3.1 Evidence that IT capabilities provided by SSC are delivered in a timely manner, on budget, and	Yes	No	Yes	No

Defence IM/IT Programme to SSC on effectiveness?	meet technical and operational requirements.				
	4.3.2 Evidence that the IT governance structure aligns SSC support requirements with SSE initiatives.	No	Yes	Yes	No
	4.3.3 Evidence that the transfer to SSC of infrastructure and applications has not affected their availability, security and condition, and that the users have access to timely and quality support services and/or operations have been running effectively.	No	Yes	Yes	Yes

Table D-2. **Evaluation Matrix—Performance (Effectiveness).** This table indicates the data collection methods used to assess the evaluation issues/questions for determining the Defence IM/IT Programme's performance in terms of achievement of outcomes (effectiveness).

Evaluation Matrix— Performance: Demonstration of Efficiency and Economy					
Evaluation Issues/ Questions	**Indicators**	**Program Administrative and Finance Data**	**Document & Literature Review**	**Key Informant Interviews**	**Questionnaire**
5.1 Is the Defence IM/IT Programme being delivered in an efficient manner?	5.1.1 Trends in expenditures over time (program costs)	Yes	Yes	No	No
	5.1.2 Operating costs	Yes	Yes	No	No
5.2 Are there more efficient ways of delivering the Defence IM/IT Programme?	5.2.1 Evidence of effective project selection and monitoring	Yes	Yes	Yes	No
	5.2.2 Evidence of timely/on budget project completion	Yes	Yes	Yes	No

5.3 What has been the impact on efficiency of transfer of services from the Defence IM/IT Programme to SSC?	5.3.1 Percentage of services delivered by SSC	Yes	No	Yes	Yes
	5.3.2 Evidence of more efficient program services/outcomes due to transfer of services to SSC	Yes	No	Yes	Yes

Table D-3. Evaluation Matrix—Performance (Efficiency and Economy). This table indicates the data collection methods used to assess the evaluation issues/questions for determining the Defence IM/IT Programme's performance in terms of efficiency and economy.