National Defence / Défense nationale

Chief Review Services / Chef - Service d'examen

CRS / CS Ex

Audit of IM/IT Framework to Support Transition to SSC

March 2015

7050-66 (CRS)



Canada

Table of Contents

Acronyms and Abbreviations

ADM(IM)	Assistant Deputy Minister (Information Management)
DBA	Database Administration
DND	Department of National Defence
DND/CAF	Department of National Defence and Canadian Armed Forces
FY	Fiscal Year
GC	Government of Canada
IM/IT	Information Management and Information Technology
IT	Information Technology
OPI	Office of Primary Interest
SSC	Shared Services Canada

Results in Brief

Assistant Deputy Minister (Information Management) (ADM(IM)) is the functional authority for information management and information technology (IM/IT) in the Department of National Defence (DND). However, the management of IM/IT in the Department is distributed amongst various organizations in addition to ADM(IM). This decentralized approach to delivering IM/IT services enables a department of this magnitude and complexity to meet specific IM/IT operational needs in an agile manner.

Overall Assessment

While some aspects of governance, control, and risk management mechanisms within DND's IM/IT framework were either implemented or in the process of being implemented, improvement is still required to support the effective transition of IM/IT to SSC.

On August 4, 2011, the Government of Canada (GC) created a new department called Shared Services Canada (SSC) to provide common IM/IT infrastructure and services and reduce duplication across departments. Given the amount of autonomy organizations within DND had over their IM/IT infrastructure and services, it has been, and continues to be, challenging for DND to transition to the common IM/IT infrastructure and IT service management practices that SSC is attempting to implement. Since SSC took control of specific departmental IM/IT infrastructure and services on April 1, 2012, any delay in the integration between the Department and SSC could impact DND's ongoing operations.

The objective of this audit was to assess whether governance, control, and risk management within DND's IM/IT framework support an effective transition to SSC services.

Findings and Recommendations

Service Transition Governance. For the most part, roles and responsibilities relating to the transition of services to SSC were not defined at the operational levels in DND. The Department has been working with SSC on clarifying its role in regard to IM/IT service delivery through formal mechanisms such as agreements and protocols, as well as attempting to align aspects of its IT service management model to that of SSC. Although the DND IM/IT change management process includes the integration of SSC, roles and responsibilities have not been formalized, thus creating a risk of unauthorized or undocumented changes. Current policy does not explicitly define the roles and responsibilities for decentralized organizations within DND to manage their own IM/IT systems and services. Without such policy instruction, it may be more challenging for DND and ADM(IM) to plan, communicate, coordinate, and implement departmental IM/IT objectives and initiatives.

It is recommended that ADM(IM) ensure that roles and responsibilities for IM/IT and organizational changes are clearly defined, communicated, and their implementation monitored.

Service Level Management. In the absence of departmental standards for documenting key service information, there was inconsistency in the structure and documentation of the services examined. This has created difficulties in aligning internal services to those of SSC and measuring service performance across the Department. It was noted, however, that most of the seven DND service provider units examined had transitioned, or were transitioning, to a DND-

wide service desk tool for service requests and service management that would help streamline services.

During the scope phase of this audit, it was challenging for ADM(IM) to determine the service level requirements, service level targets, performance evaluation, and reporting requirements for services across the Department. Nonetheless, the IT service management initiative has made progress in developing service level targets for DND national services. Service level requirements and targets are important as they represent client needs and business requirements and provide the ability to monitor performance of IM/IT services across the Department.

It is recommended that ADM(IM) develop clearly defined service level management standards for IM/IT and ensure they are monitored.

Service Knowledge Management. ADM(IM) does not have a system to manage data and information related to IT service management. Moreover, the present decentralized model for IM/IT service delivery has resulted in service information held by the various DND IM/IT service providers that is inconsistent and not easily accessible. This makes it challenging to have a comprehensive view of departmental IM/IT information that may assist in the transition to SSC and be used for decision making.

One tool that could help DND manage internal IM/IT services and help ensure that SSC and DND services are meeting client needs is a service catalogue. A service catalogue could include information about business owners and units, the impacts of incidents or changes on the business, business priority, and service levels. While a service catalogue did exist in the Department, it only included a service description and its high-level service owner. Additionally, the service catalogue was also not linked to a client portfolio that defines clients and their requirements.

It is recommended that ADM(IM) develop strategies and policy direction to ensure there is a common approach to recording, storing, and sharing service information.

Integrated Risk Management. The Department has outlined transition risks and mitigating activities at a very high level in some corporate documents. Informal risk management practices are taking place within DND to manage the transition and its impact on ongoing IM/IT operations. However, there was no evidence of formal, cohesive, and consistent risk management practices that identify, assess, and manage risks. These observations and potential improvements were discussed with management; however, no recommendation is deemed necessary in this report.

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

1.0 Introduction

1.1 Background

In 2014, the Defence Team was comprised of approximately 67,000 military members and 23,000 civilian employees.[1] Defence Team members work not only in the National Capital Region but also in other locations, such as various bases and units in Canada, the United States, and Europe, as well as other international locations supporting deployed operations, allied missions, and joint training exercises. Such a dispersed and constantly evolving organization presents a unique IM/IT challenge.

ADM(IM) operates as both the authority for IM/IT within DND and an IM/IT service provider (workstations, computer application software, classified networks, etc.) to end users in the Department. Through departmental policy, other organizations within DND have also been given authority to deliver IM/IT services, as required, creating a decentralized service model.

As a result, various organizations within DND were providing many of the same services within their respective organizations. On August 4, 2011, the GC created SSC to fundamentally transform how the Government manages its IT infrastructure,[2] and consequently some of these services are now the responsibility of SSC.

SSC provides IT infrastructure to DND and 42 other federal departments. On November 15, 2011, the GC announced that control and supervision of a large portion of budgets, people, assets, and contracts for IT infrastructure and services would be transferred from these departments to SSC by April 1, 2012. As a result, during fiscal year (FY) 2012/13 DND transferred approximately $306 million and 761 staff members to SSC.

This expectation to transition to SSC's service model by April 1, 2012 posed a significant challenge for a department of DND's size, complexity, geographical dispersion, and decentralized IM/IT organizational structure. Any attempt to continue to transition after April 1, 2012 would have had to be accomplished with limited IM/IT resources as many of these resources were transferred to SSC at that time.

With the authority granted to various organizations through the Department's decentralized approach, each organization may have their own way of managing the same IM/IT services and systems without much department-wide visibility by ADM(IM). Therefore, additional complexity was introduced as SSC had to integrate with multiple service provider organizations for the same services within DND. Figure 1 depicts the partnership between SSC and DND.

[1] FY 2013/14 Departmental Performance Report. Regular force and civilian full-time equivalents.
[2] SSC mandate. http://www.ssc-spc.gc.ca/pages/mndt-eng.html.

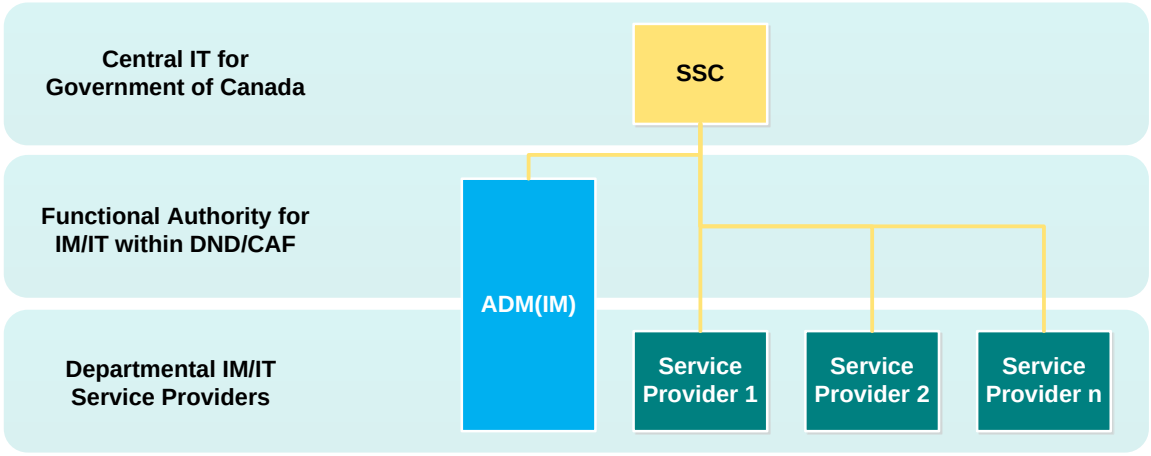

Figure1. Partnership between SSC and DND. The above diagram shows the partnership between SSC and departmental IM/IT service providers. SSC provides direct service to the IM/IT service provider(s) in each organization.

Although DND has proposed a segregation of service responsibilities document to SSC in order to maintain IM/IT operational levels within the Department, management reported that it had yet to reach an agreement with SSC. This has created challenges in advancing service integration between the two departments and has impacted DND's ability to identify, prioritize, and transition the IM/IT services requiring integration with SSC. As of March 31, 2014, the only document that had been signed by SSC and DND was a business arrangement that describes the ongoing relationship between SSC and partner organizations in general terms. While the business arrangement is the overarching component of the partner framework, special arrangements between DND and SSC and expected service performance have not yet been established.

1.1.1 DND Initiatives to Improve the Transition to SSC

DND is working with SSC to improve the integration of services between the departments. For example, DND is expanding information in its service catalogue and creating an initiative to help ensure the availability and integrity of key network services. DND management has stated that meetings have been held between the two departments regarding incident management and that an SSC operations manager has been embedded within DND to help better understand operations and requirements.

DND has developed a document that details the protocols to be used to meet its business needs. DND has also made progress in identifying IT security assets that could be transferred or shared between DND and SSC. Lastly, ADM(IM) is in the process of planning and developing measurable IM/IT roadmaps to support cyber/IT security objectives.

1.2 Rationale for Audit

During the conduct of a Chief Review Services planning study presented to the Departmental Audit Committee in March 2013, DND management identified the GC's common IT infrastructure service delivery model as a risk area. Specifically, there was concern about the impact of the transfer of certain IM/IT responsibilities to SSC. An audit of the DND's IM/IT

framework, with a scope that focuses on DND-SSC interrelated services, was identified in the Chief Review Services Risk-based Audit Plan for FY 2013/14 to FY 2015/16.

1.3 Objective

The audit objective was to assess whether governance, control, and risk management within DND's IM/IT framework support an effective transition to SSC services.

1.4 Scope

The audit scope included an assessment of the corporate functions within DND from FY 2011/12 to FY 2013/14 related to the IM/IT service delivery areas that would integrate with SSC. The timeline for the sample of IM/IT service operations was extended to December 2014 to validate test results.

Classified infrastructure and its related services were not examined because at the time the audit was initiated, it had yet to be determined if they would be part of the SSC transition. IM/IT security was also not examined as it is expected to be addressed in future audits. Lastly, the audit scope did not include examining SSC's service delivery management strategies or performance.

1.5 Methodology

The following methodology was used to conduct the audit:

- Reviewed and analyzed relevant GC and DND policies and directives, organizational business plans, corporate risk profiles, and documentation from the DND IT service management initiative;
- Reviewed and analyzed various briefings, reports, committee meeting minutes, and working group minutes;
- Conducted interviews with various stakeholders responsible for IM/IT governance and the management and provision of IM/IT services and systems;
- Analyzed a sample of 11 out of 419 approved requests for changes[3] to determine the extent of SSC's involvement in the request for change process and if SSC roles and responsibilities are in line with DND policy and guidance; and
- Selected a sample of seven database administration (DBA) service units from several different service providers to determine if the service activities performed were consistent across various service units within the Department and if information was consistently documented.

1.6 Audit Criteria

The audit criteria can be found at Annex B.

[3] A request for change is a document that requests an adjustment to a system, such as the relocation of IT infrastructure, new server approval, network access, etc.

1.7 Statement of Conformance

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

2.0 Findings and Recommendations

2.1 Service Transition Governance

While some elements of IT service management governance exist to support the transition to SSC services, DND has not fully developed and implemented a governance and service transition framework to support integration with SSC services.

Change in any work place can be a complex undertaking because it often involves managing the interrelationship of changes between people, processes, and technology. This is particularly true for DND's transition of IT infrastructure management to SSC, given the scope of the change. Not only did the Department have to transfer money, people, and assets related to SSC's mandate, it also has to transition its business to adapt to the way SSC manages IT services. It has been a challenge for the Department to effectively integrate its operations with this external IT service provider given the IM/IT resources remaining after the transfer.

2.1.1 Roles and Responsibilities

Good Practice

DND has been actively engaging SSC in developing DND's strategy and governance for SSC integration. This included setting up working groups and inviting SSC to participate as a strategic member in existing committees.

As the chief information officer for the Department of National Defence and the Canadian Armed Forces (DND/CAF), ADM(IM) is responsible for the management of IT services and ensuring their alignment with business objectives and operational priorities. During the SSC transition, however, the Vice Chief of the Defence Staff issued a series of directives in order to help ensure continuity of IM/IT services. This included defining roles and responsibilities to manage components of the transition to SSC services. However, these roles and responsibilities were only outlined at senior levels of DND.

Roles and responsibilities were not defined explicitly in other policy or guidance documents or at operational levels in the Department. For example, six of the seven sampled DBA service units within DND did not have documented roles and responsibilities. DBA services were selected for sampling because responsibility for these is now shared between DND and SSC. The lack of documented roles and responsibilities may create challenges in effectively communicating DND's operational level roles and responsibilities to SSC. Documenting the roles and responsibilities and communicating them to SSC is important in order to provide integrated services to end users.

Although SSC is participating in DND's change control process for IM/IT systems, DND's policies and procedures do not formally outline SSC's roles and responsibilities. There is a high degree of interconnectivity between elements of IM/IT systems. As such, there is a potential that changes in one component could negatively impact other systems. Without defined roles and responsibilities, there is a risk that unauthorized or undocumented changes are being implemented that may have an unintended impact on other DND IM/IT systems.

2.1.2 Transition Communication and Strategy

Effectively communicating organizational change is important in order to ensure stakeholders will understand and adopt the changes. As such, department-wide communications need to be clear, consistent, timely, and targeted to the right people. Formal communications plans could be used to ensure success of communication and stakeholder buy-in for organizational change.

There was no evidence of a department-wide communications plan. Although various organizations in DND had their own communications plans to manage the transition of IT services and systems, they were missing important components. Plans could include elements such as communication objectives and desired outcomes, stakeholder considerations, and feedback metrics (for example, the percentage of respondents that have a clear idea of what is expected of them during this service transition). A department-wide communications plan could have outlined DND's strategy to align to SSC's IT service management model for stakeholders.

Good Practice

DND-wide directives and guidance communicate some of the departmental expectations and address critical issues related to the transition of systems and services to SSC.

In order to manage current operations and the future effectiveness of DND IM/IT services, ADM(IM) developed a service proposal for SSC consideration and a strategy to align DND's IT service management model to that of SSC. Although there was evidence of plans to integrate with SSC services, they did not include documents outlining all aspects of an IM/IT service and its requirements through each stage of its lifecycle, processes to ensure that service assets (such as service information, networks, software licenses, etc.) are properly controlled, or accurate and reliable information about those assets. Without such documentation, processes, and readily accessible information, DND's ability to understand and communicate its overall departmental requirements for integration with SSC may be limited.

2.1.3 Conclusion

During the transition of IT infrastructure systems and services to SSC, DND did not outline service provider roles and responsibilities, validate that communications were received and understood by stakeholders, or fully implement and document a comprehensive IT service management strategy.

Currently, policy guidance is unclear about the roles and responsibilities for organizations to manage their own IM/IT systems and services. The decentralized approach to IM/IT service management without explicit policy direction and monitoring makes it difficult for ADM(IM) to plan, communicate, coordinate, and implement DND-wide objectives and initiatives for IM/IT.

CRS Recommendation

1. ADM(IM) should ensure that roles and responsibilities for IM/IT and organizational changes are clearly defined, communicated, and their implementation monitored.
OPI: ADM(IM)

2.2 Service Level Management

DND's service level management process is not supported by the necessary documentation and service information to communicate DND's expected service performance to SSC; however, steps have been taken in this regard.

Service level management is the process responsible for ensuring that internal clients obtain the appropriate levels of service from their IM/IT service provider. This involves collecting and maintaining service information such as service level requirements from clients that could be used to negotiate service expectations with SSC.

2.2.1 Inconsistent Documentation of Service Information

There was no evidence of departmental standards for documenting key service information. In the absence of departmental standards, the same eight activities were sampled in seven DBA service units to determine if there was consistent service information across the Department. Examples of such activities could include creating, maintaining, migrating, backing up, and recovering a database. Six of the seven DBA service units performed all eight activities, and the other service unit only performed two, resulting in a total of 50 activities.

It was expected that there would be similar DBA service information documented and available for all the 50 activities examined in order to measure and compare effectiveness of service delivery across the Department. Out of these 50 activities, 25 had documentation to support the service. An analysis of this documentation revealed that there was little consistency in service information. Without policies for service information standards, services may be designed and implemented inconsistently. Inconsistent service information creates difficulties in integrating DND services with those of SSC since SSC is pursuing common standards and efficiencies for all departments.

2.2.2 Service Information

Service level targets are based on service level requirements,[4] which represent client requirements for a particular IT service. They can be used by service providers to measure service performance and to manage client expectations of that service. These targets could also be used by DND to negotiate service expectations with other service providers such as SSC.

Good Practice

Some work has been done by the IT service management initiative to develop service level targets for DND national services. As well, a DND-wide service desk tool has been established that could monitor service response times from SSC.

[4] Information Technology Infrastructure Library definition: Service level requirements are based on client business objectives. They are used to negotiate agreed upon service level targets between the service provider and the client.

In the sample of seven DBA service units examined, there was no evidence of service information, such as service level requirements, service level targets, performance evaluations, or reporting requirements.

Overall, it was apparent during the audit that service information could not be used to assess DND's historical service performance. This is significant as common service targets and historical measures of service performance could have been used to negotiate expected levels of service from SSC.

2.2.3 Conclusion

The required standards to implement some key components of service level management, such as gathering service requirements and information and monitoring service performance in the Department, are not in place. This has resulted in inconsistent service information that may hinder DND's ability to integrate its IT services with those of SSC. Additionally, DND is not able to measure IM/IT service performance across the Department and use this information to negotiate service levels with SSC.

CRS Recommendation

2. ADM(IM) should develop clearly defined service level management standards for IM/IT and ensure they are monitored.
OPI: ADM(IM)

2.3 Service Knowledge Management

DND strategies, systems, and processes that would contribute to the effective management of service data, information, and knowledge to support integration with SSC services were generally not established.

Service knowledge management is a process that involves sharing perspectives, ideas, experience, and information and ensuring that these are readily available and accessible. The knowledge management process promotes the recording of IM/IT information in a standardized format so that it can be easily compiled and analyzed, resulting in more current, complete, and valid departmental IM/IT information. If service information is structured and documented consistently and can be accessed and shared by all relevant stakeholders, DND could reduce duplications of effort across the Department. This would enable DND to have a department-wide view of a service and be able to more effectively respond to emerging risks and more efficiently comply with policies and other legal requirements such as the transition of services and systems to SSC.

2.3.1 Accessibility of Stored Service Information

ADM(IM) did not establish governance or controls for service knowledge management within the Department. This would include creating and implementing policies, processes, and/or procedures required to maintain IM/IT data and information and make it available to those requiring it for decision-making purposes.

Also, ADM(IM) does not have a system that manages data and information related to IM/IT services and systems, and it may not have access to any of this information that exists across DND IM/IT service providers. During the audit, this information was generally difficult to locate as it was either saved on individuals' computers or on a departmental document sharing software with inconsistent naming conventions and locations. Furthermore, information that is commonly used to manage IM/IT services and assets, such as software information, process documentation, service requirements, and agreements, was not consistently available among service providers. For example, of the seven DBA service units sampled, stored information was not available for service requirements and service targets in all cases, database software assets in four cases, and documented service processes in four cases. In order to address some of these issues, ADM(IM) is planning to house hardware and software information for commonly held IT assets within DND through a recently implemented department-wide service desk tool.

2.3.2 Service Catalogue and Client Portfolio

DND recently implemented a service catalogue[5] of user, technical, and support services. However, information about those services only included a service description and its high-level service owner. A service catalogue could include, for example, information about business owners and units, the impacts of incidents or changes on the business, business priority, and service levels. As such, during the examination phase of the audit, it was difficult to link services to service providers in regions without going through a lengthy process of contacting subject matter experts or managers in the chain of command. SSC may have similar difficulties in cases where it is required to engage with DND service providers.

Good Practice

Although the DND service catalogue is not yet complete, significant work and progress has been made to implement the common service offerings listed in the catalogue for use across the Department.

DND did not have a client portfolio[6] for its IM/IT services. Such a portfolio would link clients to services, identify the decision-making authority on specific services required in the Department, and define the use and value of each service. Without policies and standards that require explicit definitions of authorities, roles and responsibilities, and documentation requirements to manage IM/IT services in DND, an accessible client portfolio with this information would have been difficult to establish. Linked client and service information would allow DND to better understand the impacts of SSC IT infrastructure changes to DND clients. The documented use and value of services to clients would allow DND to better prioritize departmental services and systems in aligning them to SSC services. Thus, ADM(IM) has begun managing priorities for IM/IT solutions that require DND and SSC services.

[5] Information Technology Infrastructure Library definition: – Service catalogue – a database or structured document with information about all live IT services, including those available for deployment.
[6] A client portfolio is a database or structured document used to record all clients of the IT service provider for IT service management in the Department and is a profile of the clients who receive services from the IM/IT service provider.

2.3.3 Conclusion

Due to the lack of strategies and policies for maintaining and managing IT service information and knowledge, information about services and service assets was not comprehensive, readily accessible, or linked to client information. These aspects are important to determine and communicate the impacts of SSC services on DND service providers and end users.

CRS Recommendation

3. ADM(IM) should develop strategies and policy direction to ensure there is a common approach to recording, storing, and sharing service information.
OPI: ADM(IM)

2.4 Integrated Risk Management

Although DND has addressed risk areas through corporate documentation and informal practices, potential improvements were discussed with management to formalize an integrated risk management approach.

Integrated risk management promotes a continuous, proactive, and systematic process to understand, manage, and communicate risk from an organization-wide perspective in a cohesive and consistent manner. It should support strategic decision making that contributes to the achievement of an organization's overall objectives.[7]

Although some corporate documents identified transition risks at a high level along with the mitigating activity, there was no evidence of a risk register to list, categorize, and rank all significant risks associated with the SSC service transition and their ongoing management. Without accessible service information from other service provider organizations in DND, ADM(IM) cannot perform a comprehensive risk assessment related to the SSC transition.

Nonetheless, there was evidence of risk being managed informally. Organizations and managers in the Department reacted to risks as they emerged through their own experience and expertise. For example, there was evidence of some action items addressing risk in a series of minutes for working groups and committees responsible for managing some components of the SSC transition; however, those risks were not always explicitly stated.

Because ADM(IM) has addressed areas of risk despite not having a formal integrated risk management approach, observations and potential improvements were discussed with management, and no recommendation is deemed necessary in this report.

[7] Treasury Board of Canada Secretariat. Guide to Integrated Risk Management. http://www.tbs-sct.gc.ca/tbs-sct/rm-gr/guides/girm-ggirpr-eng.asp.

3.0 General Conclusion

Overall, the governance, control, and risk management mechanisms within DND's IM/IT framework require improvement to increase the effectiveness of IM/IT services and to ensure the Department is adequately positioned to continue to support the effective transition to SSC services.

DND uses a decentralized approach to manage its IM/IT services and systems. This approach is complex and, in the absence of strong governance and controls, has created challenges when trying to integrate departmental IM/IT services with those of SSC. DND has actively managed the administrative and organizational complexities of the service transition through various directives and committees, but would benefit from more clearly defined roles, responsibilities, and processes for its own IT service management administration. Such processes include the development and implementation of common approaches to record, store, and share service information in order to make more decisions about services more efficiently.

The Department has been able to collect and aggregate service information through information requests and engagement with organizational clients, but only from higher levels of the organization. However, inconsistencies in how services are structured and documented and the types of service information collected make it difficult for the Department to communicate existing service requirements and service level information to SSC.

Corporate documents identified transition risks and their mitigating activity at a high level. However, a formal integrated risk management framework including a risk register, the prioritization of risk, and applicable risk management strategies did not exist. This was discussed with management and no recommendation is deemed necessary in the report.

The recommendations are provided to enhance the governance, controls, and risk management to support effective management of IM/IT services within the Department and the transition of services to SSC.

Annex A—Management Action Plan

CRS uses recommendation significance criteria as follows:

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

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

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

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

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

Service Transition Governance

CRS Recommendation (High Significance)

1. ADM(IM) should ensure that roles and responsibilities for IM/IT and organizational changes are clearly defined, communicated, and their implementation monitored.

Management Action

ADM(IM) agrees with this recommendation and is actively pursuing its implementation as follows:

a. ADM(IM) is currently conducting an analysis of the roles and responsibilities within its organization. The resulting report will detail the authorities, responsibilities, and accountabilities of the key Defence chief information officer roles. Once completed, this analysis will be extended into the operational organizations involved in SSC transition activities. This will identify which elements of ADM(IM) will be affected by the transition, what their current responsibilities are, and how these responsibilities will be altered as a result of the service transition (anticipated completion FY 2015/16); and

b. ADM(IM) is developing an operating protocol between the DND/CAF and SSC, the purpose of which will be to ensure that the specific business and program considerations that relate to DND/CAF's unique operating requirements are accommodated. This will enable both the DND/CAF and SSC to deliver their respective programs and services effectively and efficiently, while remaining compliant with their respective mandates, legal requirements, policy obligations, and management controls. This protocol sets out mutually agreed upon working arrangements to achieve this aim. In addition, the protocol includes a placeholder for the subsequent development of more detailed service level agreements that will be developed under the protocol's framework and that will further define the DND-SSC relationship. The protocol has been agreed to at the staff level between SSC and DND and is now undergoing final review (anticipated completion FY 2015/16).

OPI: ADM(IM)
Target Date: March 31, 2016

Service Level Management

CRS Recommendation (High Significance)

2. ADM(IM) should develop clearly defined service level management standards for IM/IT and ensure they are monitored.

Management Action

ADM(IM) agrees with this recommendation and is actively pursuing its implementation as follows:

a. The IT Service Management initiative, under the stewardship of Defence Renewal, will transform the manner in which IT services are managed and delivered across the DND/CAF, standardizing IT Service Management tools and processes, and delivering an enterprise IT service catalogue capability. An optimized IT environment will be achieved through the consolidation of the DND/CAF's IT service provision units into 22 or fewer Regional Service Management Centres, supported by a National Service Management Centre. From this, ADM(IM) will achieve greater central visibility, oversight, and the mechanisms required to effectively exercise functional authority. The ongoing IT Service Management initiative is anticipated to be completed in FY 2018/19.

b. In specific reference to service level management standards and their monitoring, the following actions will be taken:

   Enterprise service level management products, such as IT service catalogues, service level targets, the Enterprise IT Service Agreement, and templates for regional service level agreements, will be initiated in FY 2015/16 in support of the anticipated launch of the lead Regional Service Management Centre and the National Service Management Centre.

   i. Accountability within the National Service Management Centre for the enterprise service level management-related practices will be established in the third quarter of FY 2015/16;

   ii. Service level management processes and frameworks for the ongoing oversight, integration, and evolution of service agreements, service catalogues, service level targets, and the associated performance metrics and reporting will be initiated in FY 2016/17; and

   iii. All of the above elements will continue to evolve, transform, and align to the changing landscape as Regional Service Management Centres are established. Steady state products will be realized by project completion in FY 2018/19.

OPI: ADM(IM)
Target Date: March 31, 2019

Service Knowledge Management

CRS Recommendation (High Significance)

3. ADM(IM) should develop strategies and policy direction to ensure there is a common approach to recording, storing, and sharing service information.

Management Action

ADM(IM) agrees with this recommendation and is actively pursuing its implementation as follows:

a. The DND/CAF will transition to a common approach to recording, storing, and sharing service delivery information through an improved IT Service Management environment that will do the following:

   i. Consolidate DND/CAF's service provision units and support teams into a streamlined set of 22 or fewer Regional Service Management Centres supported by a more streamlined IT organizational model. All Regional Service Management Centres will be under the technical control of ADM(IM) as the national service management authority (anticipated completion FY 2019/20). Note that establishing the national service management authority will be dependent upon ADM(IM) being able to source the necessary personnel, which has yet to be determined;

   ii. Define and catalogue IT services common across the enterprise (anticipated completion FY 2015/16);

   iii. Establish common, universal IT service delivery processes (anticipated completion FY 2018/19); and

   iv. Implement a common supporting toolset (anticipated completion FY 2015/16).

b. For business related data and information, the DND/CAF has issued DAOD 6001-1 – Recordkeeping, which directs that record management practices must be employed on this type of information. For service information specifically, there are currently two DAODs in development on the topics of IT service management and IT service support.

OPI: ADM(IM)
Target Date: March 31, 2016 to March 31, 2020

Annex B—Audit Criteria

The audit criteria were assessed using the following levels:

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

Governance

1. **Criteria.** DND has developed and implemented a governance and service transition framework to support integration to SSC services.

   Assessment Level 4 – While some elements of IT service management governance exist, there is a disparity between DND's decentralized authority for IM/IT system and service management and policy direction that will help ensure the Department can coordinate and support the integration to SSC services.

Internal Control

2. **Criteria.** Strategies, systems, and processes are in place to effectively manage service data, information, and knowledge to support integration to SSC services.

   Assessment Level 4 – Information for IM/IT services, which would support decisions about how DND is integrating its IM/IT services with SSC was not readily available.

3. **Criteria.** A process is in place and is effective in identifying, communicating, and measuring satisfaction of SSC service requirements.

   Assessment Level 2 – There is a process in place to identify, communicate, and measure satisfaction of SSC service requirements. The process could be improved by having more clearly defined DND IM/IT services. As this process requires relatively minor improvement, observations and recommendations for this area have been briefed to ADM(IM).

4. **Criteria.** DND service level supports current and planned IM/IT services falling under the SSC services mandate to deliver agreed upon and achievable targets.

   Assessment Level 4 – Although ADM(IM) has taken steps toward developing common service expectations, management of IM/IT activities within DND does not fully support the development of agreed upon and achievable targets with SSC.

Risk Management

5. **Criteria.** DND's transition to SSC services is appropriately risk managed.

   Assessment Level 2 – Although ADM(IM) did not formally identify, assess, and manage risks of the SSC integration to support efficient and effective delivery of IM/IT services, it did manage risks informally through various governance committees and working groups and reflected it in corporate documentation. Since this process requires minor improvement, observations and recommendations for this area have been briefed to ADM(IM) and are not included in the report.

Source of Criteria

1. Treasury Board Secretariat, Audit Criteria Related to the Management Accountability Framework: A Tool for Internal Auditors, March 2011

   - Reference to: G-3, G-4, G-7
   - Reference to: AC-3
   - Reference to: CFS-1, CFS-2, CFS-3, CFS-4, CFS-5
   - Reference to: LICM-2, LICM-3, LICM-4
   - Reference to: RP-2, RP-3
   - Reference to: RM-2, RM-3, RM-4, RM-5, RM-6

2. Information Technology Infrastructure Library, 2011 Edition

   - Service Strategy
   - Service Transition
   - Service Design

3. Treasury Board Directive on Management of Information Technology