



Reviewed by ADM(RS) in accordance with the *Access to Information Act*. Information withheld in accordance with the AIA under sections 16(2)(c), 19(1), 21(1)(a), 21(1)(d).

Audit of Information Management



1259-3-0067 ADM(RS)
978-0-660-45019-3
D2-629/2022E-PDF
July 2022

Table of Contents

Introduction

Pages 3–10

Acronyms

Report Guide

Executive Summary

Context

Key Themes

IM Governance and Framework Implementation

Pages 11-12

Finding 1

Consideration 1

Monitoring and Change Management

Pages 13-14

Finding 2

Consideration 2

Case Study: High-Risk Activity Monitoring and Oversight

Pages 15-16

Finding 3

Consideration 3

Conclusion and Annexes

Pages 17-19

Overall Conclusion

About the Audit



Acronyms

ADM(DIA)	Assistant Deputy Minister (Data, Innovation and Analytics)
ADM(IM)	Assistant Deputy Minister (Information Management)
ADM(RS)	Assistant Deputy Minister (Review Services)
ARA	Accountability, Responsibility and Authority
CAF	Canadian Armed Forces
CIO	Chief Information Officer
DAOD	Defence Administrative Orders and Directives
DIM Secur	Director Information Management Security
DKIM	Director Knowledge and Information Management
DND	Department of National Defence
DWAN	Defence Wide Area Network
IM	Information Management
IMO	Information Management Officer
ISSO	Information System Security Officer
IT	Information Technology
ITSS	Information Technology Security Standard
L1	Level 1
NDSOD	National Defence Security Orders and Directives
PITD	Portable Information Technology Device
RACI	Responsible, Accountable, Consulted, Informed
RDIMS	Records, Documents and Information Management System
SD	Standard Definition
SSE	Canada's defence policy: <i>Strong, Secure, Engaged</i>
TB	Treasury Board
TBS	Treasury Board Secretariat
USB	Universal Serial Bus

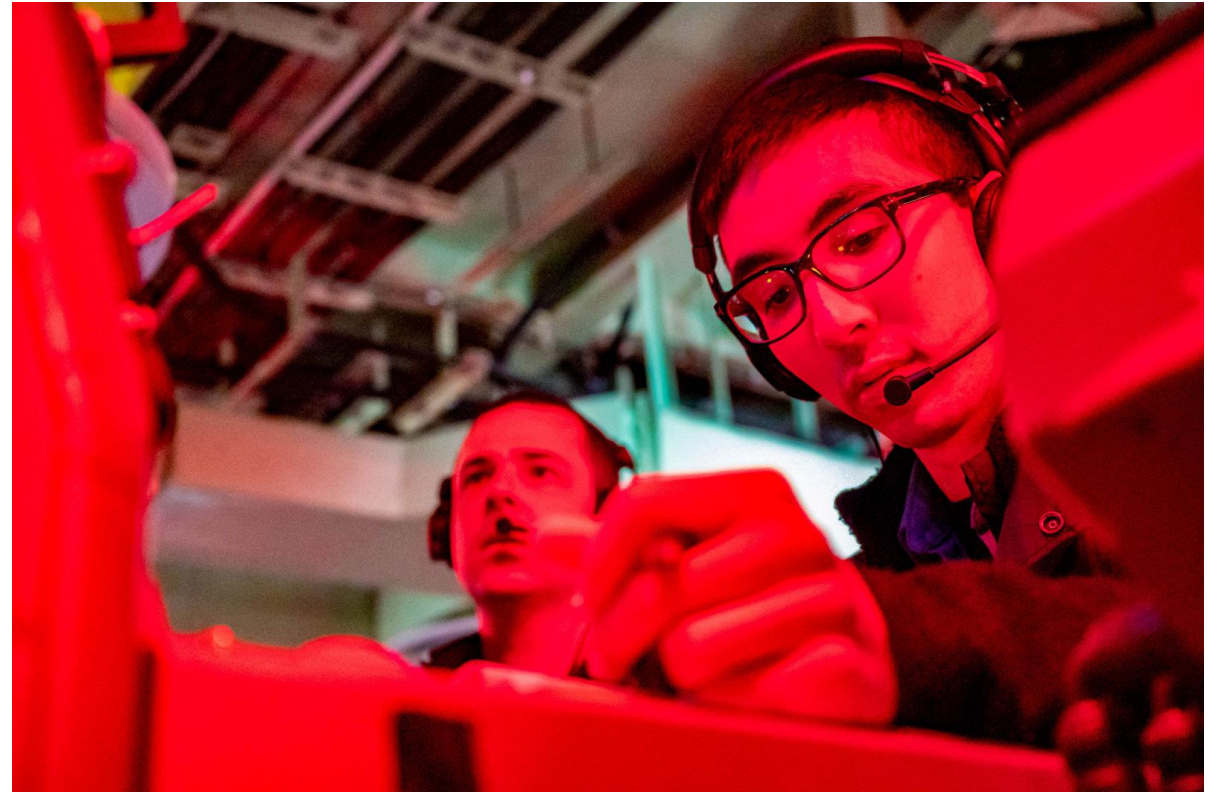


Photo Cpl Lynette Ai Dang, Canadian Forces Combat Camera 20210531PRAD0001D015

Report Guide

Here are some guidelines for navigating the document.



This document is best viewed on a device such as a laptop, desktop or tablet, as opposed to printing.



This document, if printed, should be done so in colour to maintain the integrity and intent of the graphical components.



This icon indicates an area of consideration made by Assistant Deputy Minister (Review Services) (ADM(RS)).

Executive Summary – Findings and Considerations

Table 1. Executive Summary – Findings and Considerations

FINDINGS	CONSIDERATIONS
<p>IM Governance and Framework Implementation DND has an established IM Governance structure and framework. The way ARAs are documented is fragmented. Risk management is not formally embedded in governance processes.</p>	<p>C1. A refresh of the existing IM governance structure led by ADM(IM) in collaboration with Assistant Deputy Minister (Data, Innovation and Analytics) (ADM(DIA)) is ongoing. This will help support the delivery of the Departmental IM Programme objectives and decision making. As part of this refresh, ADM(IM) should also consider opportunities to consolidate ARAs and formalize risk management and reporting.</p>
<p>Monitoring and Change Management Monitoring mechanisms to assess the implementation of the IM framework exist with limited capacity to analyze results and make substantial improvements. While components of change management and training exist, they are not well established to ensure success of new IM initiatives.</p>	<p>C2. To promote the successful implementation of future IM initiatives across the Department, ADM(IM) should consider:</p> <ul style="list-style-type: none"> • Continuing to leverage Health Check results to identify ongoing improvement opportunities; • Developing and implementing a generic change management process to be leveraged by all L1s; and • Establishing a training plan based on a training efficacy and needs analysis.
<p>Case Study: High-Risk Activity Monitoring and Oversight Information sharing and transfer protocols are established. .</p>	<p>C3. To mitigate the information security risks while enabling operational needs, ADM(IM) should consider:</p> <ul style="list-style-type: none"> • Consulting with all L1s to establish internal and external information sharing and transfer requirements; • Developing and implementing a process which enables information to be shared, transferred and monitored in a timely manner; and • Examining through on-going modernization initiatives, automated monitoring and controls capabilities while implementing new IM tools.

Context

Key Stakeholders Roles and Responsibilities

Table 2. Key Stakeholders Roles and Responsibilities.

Stakeholders	Roles and Responsibilities
Assistant Deputy Minister (Information Management) (ADM(IM))	ADM(IM), in the role of Defence Chief Information Officer (CIO), has functional authority over IM, Information Technology (IT) Management, Defence Terminology, IT Security, Communications Security and Information Security. Their mission is to deliver timely, trusted and secure information to contribute to the success of the Defence Team.
Director Knowledge and Information Management (DKIM)	DKIM is responsible for overseeing the DND/CAF IM program and providing IM guidance and services, with the intent of managing information as a strategic resource. DKIM delivers strategic information governance, services and innovation, enabling management of information across DND/CAF, regardless of medium or format, which support business processes and decision making.
Director Information Management Security (DIM Secur)	DIM Secur oversees IT and Information Security in DND/CAF. It supports and advises on the effectiveness of IT security risk-mitigation measures through the Security Assessment and Authorization, Oversight and Compliance, and Industrial Information Security programs.
Assistant Deputy Minister (Data, Innovation and Analytics) (ADM(DIA))	ADM(DIA), in the role of Chief Data Officer, provides DND/CAF with the expertise required to enhance the Department's data and analytics capabilities, and to provide business innovation support. The DND/CAF Data Strategy provides a roadmap for public servants and military personnel to leverage data in all aspects of Defence programs, enhancing our capabilities and reporting, and providing an information advantage to our military.
Information Management Officers (IMO)	IMOs are IM functional specialists. They act as the liaison between their L1 and ADM(IM) and are advisors to their L1's senior management providing guidance on IM processes and systems. IMOs are also responsible for creating and maintaining their L1's IM plan as well as the annual monitoring requests from ADM(IM).
Treasury Board (TB) Library and Archives Canada	TB is the key policy authority for the Government of Canada <i>Policy on Service and Digital</i> , and any internal policies or guidance should align with TB Directives and Guides which are promulgated by the Treasury Board Secretariat (TBS). Library and Archives Canada provides leadership in the Government of Canada IM community by developing and providing standards, tools, best practices, advice, guidance and services.

Context

Information Management – Key Concepts

In April of 2020, TBS made major changes to the Government of Canada IM policy by publishing a new policy and directive governing IM. The new policy replaced several existing policies, resulting in DND working to update Departmental Defence Administrative Orders and Directives (DAOD) to reflect these changes. The new policy on Service and Digital focuses on the client, ensuring proactive consideration at the design stage of key requirements of these functions in the development of operations and services. It establishes an enterprise-wide, integrated approach to governance, planning and management, including integration of services such as service delivery, information and data, IT and cyber security in the digital era.

TBS defines IM as a discipline that directs and supports effective and efficient management of information in an organization, from planning and systems development to disposal or long-term preservation (**Figure 1**). Data management is the development, execution and supervision of plans, policies, programs and practices that deliver, control, protect and enhance the value of data assets. Reliable information for decision making is dependent on accurate, timely and accessible data.

IM is thus fundamental to all aspects of the Department’s business in that it supports informed decision making, efficient and effective service delivery, collaboration across organizations and is critical to achieving the goals of the Department (**Figure 2**).

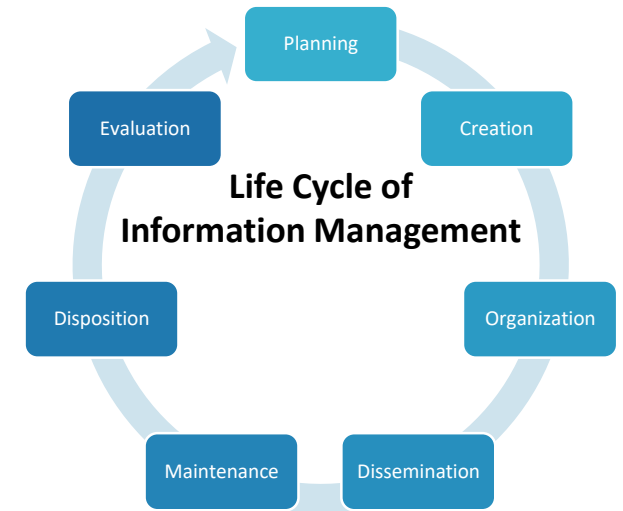


Figure 1. Life Cycle of Information Management

How Business Intelligence, Information and Data are Related

Business Intelligence

Comprises the strategies and technologies used by enterprises for the data analysis of business information.

Information

Data that is structured or presented so as to make them meaningful or useful.

Data

Qualitative/quantitative facts or Figures.

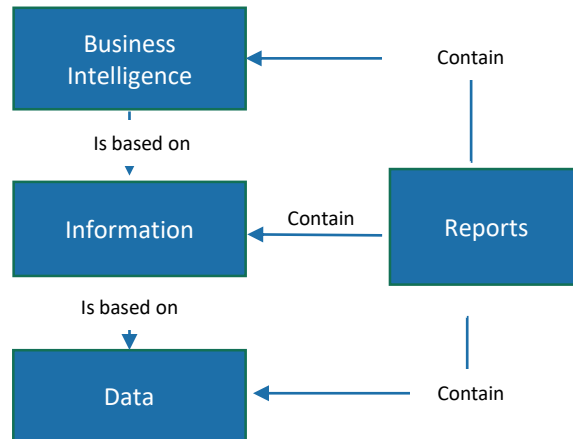


Figure 2. How business intelligence, information and data are related

Information Systems of Record

DND has several corporate repositories of information and has a number of key ongoing organizational initiatives to streamline them. The list of approved corporate repositories for DND includes; GC Docs, Records, Documents and Information Management System (RDIMS), Shared Drive, SharePoint, Microsoft 365, employee personal drives, as well as secured information systems. DND also has a substantial amount of information stored off of the approved corporate repositories in places which include; Microsoft Outlook, employee’s computer desktops, and various Portable Information Technology Devices (PITD), as well as hard copy records.

Context - continued

Defence IM Programme and Stakeholders

DND's IM Programme is led by ADM(IM), as the DND/CAF CIO, but is applied by L1 organizations across the Defence Team. Although ADM(IM) is the functional authority and holds the primary responsibility for providing IM direction, procedures and enterprise tools, they rely on L1s to develop and implement IM plans and activities within their operational areas. While the scope of this audit was focused on ADM(IM)'s IM role within DND/CAF, ADM(IM) cannot successfully execute, monitor and roll out IM initiatives without the cooperation and collaboration of other groups within the Defence Team. **Figure 3** provides a view of the key stakeholders involved in the IM programme. Policy Drivers set policies, issue direction and set conditions that directly or indirectly shape information capabilities. Service Providers conceive, design, build and/or acquire, and manage information capabilities as part of their broader activities to achieve their assigned missions and tasks. End-users define requirements and produce, disseminate and consume information as a fundamental enabler of their assigned mission or role. This illustrates the inherent complexity of aligning ARAs.

The two core documents that outline DND's principles and approach for IM are the 2019 Defence Information Strategy and the 2019-22 Defence Information Management Plan. The Strategy is aligned with the Government of Canada policy and Canada's defence policy: *Strong, Secure, Engaged* (SSE). It identifies the strategic priorities and objectives, approaches and resources to deliver information capabilities to achieve strategic, operational and tactical advantage for DND/CAF, and is aligned with the Government of Canada's plan and digital standards. The IM Plan establishes "a roadmap for the way DND/CAF leverage information and data in support of timely, efficient and effective decision making in business and operations," through six objectives and corresponding activities and performance indicators. These objectives are:

1. Strengthen the Defence IM Programme;
2. Mature IM Services;
3. Develop and Implement Standardized DND/CAF IM Reporting;
4. Drive DND/CAF Digitization;
5. Increase Participation in Open Government; and
6. Establish IM Learning and Professional Development.

Ultimately, the ideal maturity level for the Defence Team is defined as having the right information at the right time delivered to the right people, which is what the IM programme is striving to achieve.

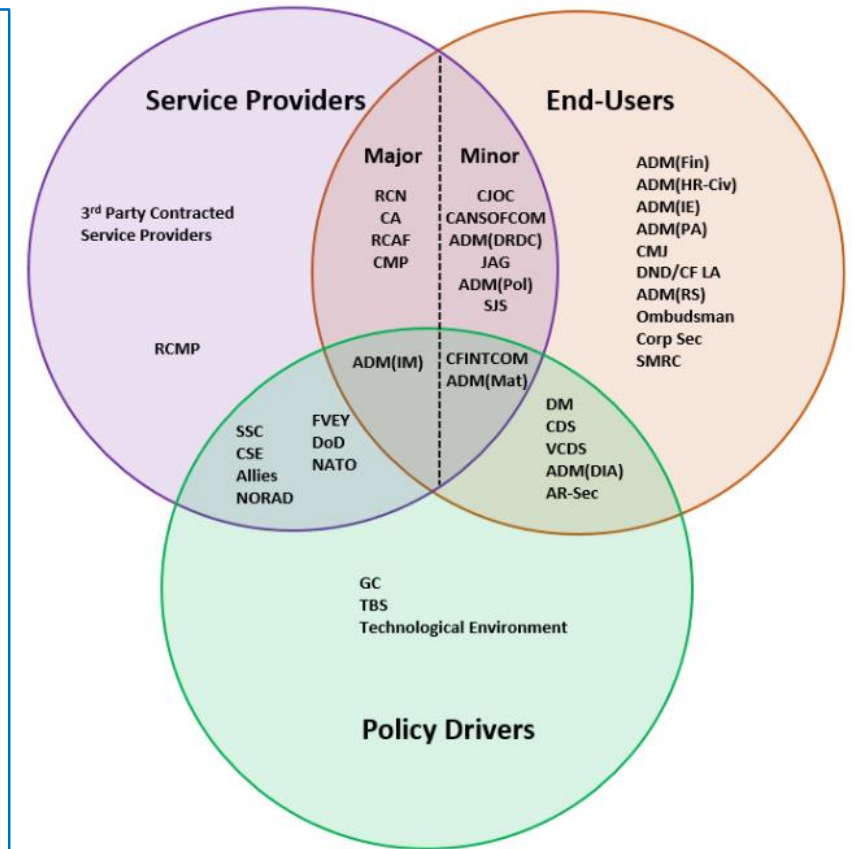


Figure 3. Defence Information Programme Stakeholder Map
Source: ADM(IM)

Key Themes

The Key Findings were aligned with three themes as follows:

1 IM Governance and Framework Implementation


2 Monitoring and Change Management

3 Case Study: High-Risk Activity Monitoring and Oversight



Master Corporal Jordan Lobb, Canadian Forces Combat Camera
20200211ISD0001D005

IM Governance and Framework Implementation

 **FINDING 1:** DND has an established IM Governance structure and framework. The way ARAs are documented is fragmented. Risk management is not formally embedded in governance processes.

Why It Matters

An effective and fully implemented IM governance framework is key to delivering on the IM Programme while supporting L1s in meeting their IM responsibilities. It would allow DND/CAF to manage information throughout its life cycle, as a valuable asset and strategic resource, to support the outcomes of programmes, services, operational needs and accountabilities. Clearly defined ARAs, as well as effective governance committees enable transparent and risk-based decision making, and are crucial to achieve IM maturity for the Defence Team. An effective IM framework also ensures that DND/CAF is in compliance with key legislative requirements and supports reporting to both internal and external stakeholders.

What We Found

The Department has an IM framework in place that includes DAODs, National Defence Security Orders and Directives (NDSOD), the Defence Information Strategy and the Defence Information Management Plan. The IM framework was found to be in line with the *TB Policy and Directive on Service and Digital* with regard to key elements including privacy, security and safeguarding of information.

The governance framework includes IM governance boards and committees which provide direction to the Defence Team and oversee IM-related initiatives. The three key IM governance bodies at DND/CAF are the Information Management Board, the Information Programme Working Group and the IM and IT Capability Development Board, primarily led by ADM(IM) as the functional authority. It was noted that two of the three committees were not fully operating as intended per their terms of reference indicating that IM matters may not be getting the level of priority and attention required. For example, the number of meetings per year did not occur as required; the records of decision were not consistently prepared and made available; and attendance by board members was inconsistent or representatives were not at the appropriate level to contribute.

While risks were occasionally discussed, there was no clear indication that risks were being managed and/or reported beyond the committee meeting. Risk management is not explicitly included in the committees' terms of reference. The lack of consideration for risks within the IM governance structure could result in risks not being identified, escalated at the right level and mitigated which could affect decision making.

IM Governance and Framework Implementation

FINDING 1: Continued

What We Found

DND/CAF has documented ARAs which support the governance structures of IM, and include descriptions for the Deputy Head, the CIO, L1s, IMOs, Managers and Commanding Officers, employees and CAF members. Although there was no overlap or duplication identified, ARAs are documented across multiple internal and external policies, making it challenging to quickly identify relevant ARAs. For any given DND initiative or project there may be multiple business owners, technical authorities, contracting authorities, project authorities or security approvers residing in various L1s. Accountability for the IM component quickly becomes a challenge within this complex landscape. A lack of clear accountability can result in gaps or duplication of effort. A RACI (Responsible, Accountable, Consulted, Informed) chart is a best practice that may provide a centralized record of ARAs.

The IMO role is important within each L1 as they are IM functional specialists. They act as the liaison between their L1 and ADM(IM) and are advisors to their L1's senior management providing guidance on IM processes and systems. They are critical to the implementation of the IM Programme and IM policy within each L1. IMOs are also responsible for creating and maintaining their L1's IM plan as well as the annual monitoring requests from ADM(IM). The Defence Team's IM Plan identifies a goal of having at least one IMO within every L1. While most L1s have an IMO in accordance with policy requirements, their duties are not always well defined, nor consistently applied across L1s. In addition, the role of IMO can be a secondary duty and assigned on a rotational basis. This results in the quality of the L1 IM plans being inconsistent, not always including measurable targets or timelines, and often unmonitored.

While DND has many key elements of a framework established, the current level of prioritization of IM is not sufficient to achieve the sought IM maturity level. Therefore, DND/CAF may be less strategic in responding to information reporting requirements and requests such as access to information and privacy requests or legislative reporting requirements. There is an expectation based on the new policy that organizations integrate service delivery, information and data, IT and cyber security in any initiative which will require clear ARAs and effective collaboration.


The Defence Information Management Planning group has identified the need to update the current IM governance structure within DND/CAF as it is acknowledged that it is not functioning as intended. The existing governance structure and processes are being assessed to determine how they can best support the roles and responsibilities of the ADM(IM) as the CIO to evaluate, direct and monitor the performance of the IM Programme.

C1



A refresh of the existing IM governance structure led by ADM(IM) in collaboration with ADM(DIA) is ongoing. This will help support the delivery of the Departmental IM Programme objectives and decision making. As part of this refresh, ADM(IM) should also consider opportunities to consolidate ARAs and formalize risk management and reporting.

Monitoring and Change Management

 **FINDING 2:** Monitoring mechanisms to assess the implementation of the IM framework exist with limited capacity to analyze results and make substantial improvements. While components of change management and training exist they are not well established to ensure success of new IM initiatives.

Why It Matters

Monitoring is required to identify areas for improvement and assess compliance. It is also a key tool to support decision making and to identify emerging risks. Finally, monitoring enables the Department to collect information to assess the IM maturity and the achievement of IM programme objectives.

The digital era requires ongoing upgrades to manage the vast quantity of information being processed in a large department such as DND/CAF. Thus, change management is required in the IM context when a new IM initiative is implemented, for instance, to support the organization and the users in their transition. Even a very well managed initiative may fail if the organization is not willing to adopt it. Effective change management is a key success factor to a large organization such as the Defence Team, supported by a robust training plan to allow change to be sustained across the organization.

What We Found

The Defence IM Plan was issued in April 2019 and covers the period from 2019 to 2022, with the next iteration expected in April 2022. The IM Plan has six objectives which support the objectives outlined in the Defence Information Strategy that ultimately support SSE. Each objective has activities and performance indicators with timelines, and are used to derive ADM(IM)s annual Health Check. The IM Health Check, introduced in 2019, is the primary monitoring initiative designed to assess the IM framework's implementation status and application across the Defence Team, and it is communicated via the functional planning guide issued to L1s. The guide also includes requirements for L1s to submit or refresh an IM Plan and to submit metrics for the IM Health Check. The process relies partly on L1 self-reporting, and ADM(IM) often lacks the capacity to review and provide comprehensive feedback to L1s based on their submissions. The Health Check establishes IM performance measures and collects information to assess IM maturity across DND/CAF. It also enables reporting against the measurable targets and timelines included in the IM plan. In addition to supporting the IM Plan and Strategy, the IM Health Check enables ongoing improvement while assessing IM maturity which is based on eight key indicators, namely: accountability; transparency; integrity; protection; compliance; availability; retention and disposition. While it showed maturity had improved between 2019 and 2020, improvement was limited. Refer to **Annex B** for maturity model.

Beyond the Health Checks that provide high-level monitoring by assessing IM maturity, limited analysis is done on IM compliance, and there is little oversight for everyday usage and recordkeeping management practices. Many practices rely on the users being aware and following the IM protocols. It is largely up to L1s to implement their own monitoring practices. To continue working towards the desired IM maturity level, ADM(IM) may need to leverage its role as functional authority to enhance and monitor IM compliance across L1s.

Monitoring and Change Management

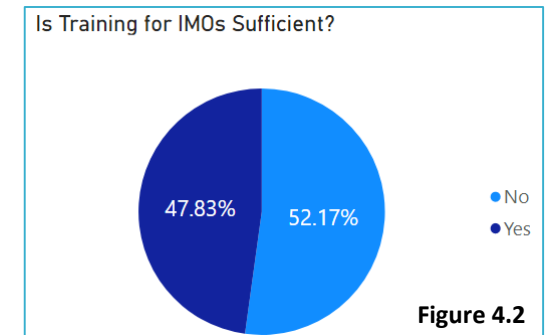
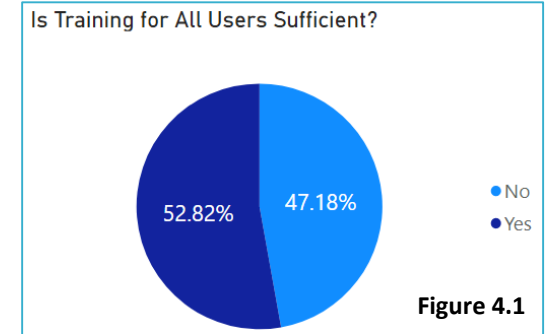
FINDING 2: Continued

What We Found

Change management is a key enabler to successfully implement IM initiatives, and it is embedded in the IM pillars. By definition, change management is about influencing the organization to effectively adopt new initiatives. While ADM(IM) has many IM services to offer to meet the Defence Team's IM needs, they face challenges with the implementation of their initiatives due to the size, complexity and mandate of DND/CAF. Lack of capacity both for human resources and funding has been highlighted as a factor. Similarly, L1s acknowledge the importance of IM but struggle with limited resources and priorities to meet their own operational requirements. An effective approach to change management and a change management process that is scalable and repeatable would better support IM initiatives roll out. ADM(IM) is in the process of designing and developing a change management process and plan. As ADM(IM) continues rolling out core initiatives, such as the enhancement of Office 365 to be used as a centralized information repository, an effective change management process will be key.

Training plays a critical role in change management as it allows users of IM products to buy-in and realize the benefits of the new process, tool or system. It also teaches users how to use the new products properly and thus helps ensure IM rules and requirements are met.

While there is a suite of IM training available, for instance multiple GC Docs trainings are required before access to the tool is granted, it was found that IMOs, employees and managers believe that current IM training is not sufficient to meet operational requirements (**Figure 4.1**). The majority of IMOs and almost half of general users do not feel they have been sufficiently trained for their role (**Figure 4.2**). IM training is considered accessible and communicated but out of date and not always timely. There is no plan or policy outlining requirements to regularly review and update training, and training efficacy is not measured. In addition, there is no requirement for ongoing or cyclical IM training post-onboarding of new employees. A training gap analysis is currently being conducted by ADM(IM) to help improve IM maturity. ADM(IM) is also currently in the process of developing an IM training plan.



- C2** To promote the successful implementation of future IM initiatives across the Department, ADM(IM) should consider:
- Continuing to leverage Health Check results to identify ongoing improvement opportunities;
 - Developing and implementing a generic change management process to be leveraged by all L1s; and
 - Establishing a training plan based on a training efficacy and needs analysis.

Overall Conclusion

An effective and well implemented IM framework is essential to DND in this digital era. There are many opportunities to maximize our delivery of operations and mandates by leveraging timely, accurate and accessible information. On the flipside, it also creates an increasingly complex landscape with associated risks that need to be well managed.

The design of DND's IM governance structure and key IM management activities support the Department's IM priorities and objectives, and align with prescribed legislative and policy requirements. Guidelines and procedures are extensive, and are consistent with the TB *Policy on Service and Digital*, with inclusion of key requirements related to privacy security and safeguarding of information. While the governance committee structure is established with multi-level governance bodies, it could benefit from formalizing its risk management practices and reporting to enable articulation and escalation of key risks and by supporting decision making. ADM(IM) has already taken steps to improve, as evidenced by the current review of their governance structure. Effective collaboration will be key in line with the requirement to integrate services with a client-centric focus articulated by the new policy. DND/CAF has documented ARAs for key IM stakeholders which need to be consolidated to better support complex and interdependent initiatives.

The IMO network has a key role to play in supporting the delivery of the IM Programme, with all L1s generally staffed with these key positions, although not necessarily to the extent required with IMOs holding multiple roles and duties. While they are essential in supporting IM compliance and meeting IM programme objectives, the IMOs largely work independently of each other, and they could benefit from additional guidance and support, in particular in the development of their IM plan. IM generally needs to be better prioritized.

With regard to monitoring and improvement mechanisms, the Health Check is the primary tool to assess the implementation of IM initiatives across the Defence Team, including IM maturity. Going forward, more can be done with Health Check results to drive ongoing improvements to achieve the sought-after IM maturity level.

The importance of change management is recognized, and is often critical to the success of any initiative, in particular large scale transformational initiatives. ADM(IM) should consider leveraging the fundamentals of change management to implement their initiatives by developing a change management process that is scalable and repeatable. Further, users and stakeholders of IM feel that they are not sufficiently trained to meet the needs of DND/CAF.

Finally, monitoring over devices that present higher security risks exists ||||| . Any information leaks or breaches can have dramatic consequences, so more work is needed to strengthen the control environment over information sharing, while still enabling operational requirements to be met.

Overall, the design of DND's IM governance structure and key IM management activities support the Department's IM priorities and objectives, and align with prescribed legislative requirements. Opportunities exist to improve the effectiveness of the governance structure and the key framework implementation components, as well as to enhance information transfer, sharing and monitoring mechanisms.

Annex A – About the Audit

The findings and recommendations of this report were derived from multiple sources of evidence collected throughout the planning and conduct phase of the project. These sources of evidence were verified with the Offices of Primary Interest to ensure their validity. The methodology used in this audit were as follows:



Document Review

The audit team completed a review of relevant internal/governmental policies, legislations, directives, communications, procedures, guidelines and templates. Documents were maintained for evidence, as required, and were substantiated with other methods of evidence collection.



Interviews

The audit team conducted interviews with key stakeholders. These responses were used to improve the team's understanding of areas of concern, existing processes and controls, and risks.



Survey

The audit team carried out a survey with a range of stakeholders with a focus on the training requirements. The results were used to substantiate document review and interview observations.

Audit Criteria

- DND has established an IM framework (including policy, governance and controls) that is aligned with legislative requirements.
- DND has implemented the IM framework across the organization.

Audit Objective

The objective of the Audit of Information Management was to determine whether current management activities and governance structures support the management of information within the Department.

Audit Scope and Timeframe

The scope of this audit included governance structures, controls and training related to information management from April 2020 to September 2021, and any Departmental initiatives related to IM. The audit included various L1s to test the application of the IM framework and included both digital and paper information management.

Conduct work started in September 2021 and was substantially completed in March 2022.

Scope Exclusion

The scope of the audit excluded:

- Risk of insider threats and leaks of information;
- Quality of information and data for decision making;
- Classified IM and/or IT systems, documents and material; and;
- Testing of IT system access and security controls.

Statement of Conformance

The audit findings and conclusions contained in this report are based on sufficient and appropriate 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.

Annex B – International Information Governance Maturity Model

1 Sub-Standard	2 In Development	3 Essential	4 Proactive	5 Transformational
<p>Recordkeeping concerns are either not addressed at all, or are addressed in a very ad hoc manner.</p>	<p>Developing recognition that recordkeeping has an impact on the organization, and that the organization may benefit from a more defined information governance program.</p>	<p>Defined policies and procedures, and more specific decisions taken to improve recordkeeping.</p>	<p>Information governance issues and considerations are integrated into business decisions on a routine basis, and the organization easily meets its legal and regulatory requirements.</p>	<p>Integration of information governance into organization overall corporate infrastructure and business processes to such an extent that compliance with the program requirements is routine.</p>
<p>Organizations should be concerned "that their programs will not meet legal or regulatory scrutiny."</p>	<p>Organizations are "still vulnerable to legal or regulatory scrutiny since practices are ill-defined and still largely ad hoc in nature."</p>	<p>Organizations "may still be missing significant opportunities for streamlining business and controlling costs."</p>	<p>Organizations "should begin to consider the business benefits of information availability in transforming their organizations globally."</p>	<p>Organizations "have recognized that effective information governance plays a critical role in cost containment, competitive advantage, and client service."</p>

(Applying ARMA International Information Governance Maturity Model)