

January 2023

Audit of Information Management

Audit and Evaluation Division



Veterans Affairs
Canada

Anciens Combattants
Canada

Canada

Acknowledgements

The audit team gratefully acknowledges staff members from Veterans Affairs Canada, and employees from Statistics Canada, Royal Canadian Mounted Police, Canada Border Services Agency, and Library and Archives Canada. Their contributions were essential to the success of this audit.

Table of Contents

1.0 BACKGROUND.....	1
2.0 ABOUT THE AUDIT	2
3.0 AUDIT RESULTS.....	4
4.0 AUDIT OPINION.....	11
APPENDIX A - AUDIT CRITERIA	13
APPENDIX B - METHODOLOGY	14

1.0 Background

The Audit of Information Management was approved by the Deputy Minister as part of the 2021-23 Risk-Based Audit Plan.

In the Government of Canada, information is safeguarded as a public trust and managed as a strategic asset to maximize its value in the service to Canadians. The vision is achieved through the implementation of the Government of Canada Information Management Strategy and associated policy instruments, including the *Policy on Service and Digital*.

Information management is 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. The focus of information management is the ability of organizations to capture, manage, preserve, store and deliver the right information to the right people at the right time. The Department produces a vast array of information, including data, documents, graphics, recordings, videos, photographs, and social media posts. With advances in technology, the amount of information, and digital information, in particular, continues to grow exponentially each year. Storage options (e.g., cloud) are scalable, making it easier and cheaper to store large volumes of information.

Veterans Affairs Canada has a centralized Information Management (IM) unit within Head Office, which ensures that the responsibilities are met.

The main activities of the VAC IM team consist of the following¹:

- Establishing Information Management governance.
- Developing policies, procedures and guidelines in support of Information Management policies and central agency requirements.
- Promoting awareness of information management best practices and procedures to ensure employees understand their roles and responsibilities.
- Providing VAC staff with advice, guidance and training on Information Management.
- Directing and supporting efficient and effective information management during project planning and systems development.
- Supporting VAC in meeting its commitments to openness and transparency.

More specifically, the VAC IM Team provides expert services to support effective and coordinated management of information within the Department. These services include:

- Records Lifecycle Management (paper and electronic)

¹ [Information Management - VAC@work \(vac-acc.gc.ca\)](#)

- Library management and research
- Direction, advice and guidance on:
 - How to file, organize and store paper and electronic information
 - Where, how and for what period of time information should be kept
 - Disposal of information
 - What decisions and actions must be documented, and what information has business and archival value
 - IM requirements in Statements of Work, Contracts and Privacy Impact Assessments
 - Leading IM practices to ensure consistent, effective and efficient use of information
- IM Awareness and training, including GCdocs² training
- Implement and monitor policies, standards, principles and practices to ensure Departmental compliance with Treasury Board Secretariat and Library and Archives Canada direction
- Identification and transfer of archival records to Library and Archives Canada for long-term preservation
- Participation in project planning and initiatives to identify information management requirements
- Oversight and operations of GCdocs as the corporate repository of information
- Implementation of Open Government³

Ensuring information is appropriately maintained and stored allows for good governance, informed decision making and the efficient and effective sharing of public information.

2.0 About the audit

2.1 Audit objectives and scope

Audit objectives:

The objective of this audit was to provide reasonable assurance that adequate governance monitoring frameworks were in place to ensure the successful management of information at Veterans Affairs Canada.

² GCdocs is a web-based tool and an official repository used for managing, organizing, and sharing electronic information in the Government of Canada.

³ Open Government is about making government more accessible to everyone. Participate in conversations, find data and digital records, and learn about open government.

More specifically, the objective was to provide reasonable assurance that:

- VAC has implemented an effective management control framework which includes accountability, roles, responsibilities, and monitoring to mitigate information management risks; and
- VAC has implemented effective operational and technical controls through the organization which includes recordkeeping methodologies and tools, as well as awareness and training activities to mitigate risks related to Information Management.

Scope:

Information Management is a vast topic with many different layers. The scope of this audit included the information management and governance control frameworks in place at VAC on 1 January 2020 up to and including 30 September 2021. Covering this time period, the Audit Team focused on the main activities of the VAC Information Management team as described above in the background section. The audit scope did not include a focus on the security of systems that manage information as it relates to vulnerability from outside attacks such as cyber-attack threats. In addition, this audit concentrated on the management of corporate information and not Veteran related information.

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 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.

Additional information including the audit criteria and methodology are provided in Appendices A and B.

3.0 Audit results

3.1 Information management governance framework

A governance framework contains the practices and procedures that are reasonably expected to be in place in any department or agency to enable the achievement of objectives. These practices help create business value and minimize risk for the organization. They include policies, procedures, business processes, roles and responsibilities, objectives and/or performance measures, monitoring and reporting.

An effective framework supports the organization's ability to manage risks and to achieve objectives related to operational effectiveness and reliable reporting. It is important to note that a framework would not guarantee that risks will be prevented, detected and managed, nor that the organization will achieve its goals. It does, however, greatly increase the likelihood that organizational risks will be mitigated, and objectives will be achieved⁴.

From an information management perspective, this should mean that important information is properly maintained and stored and is readily available to guide and support informed and effective decision making.

3.1.1 Roles and responsibilities

Why it's important

At the outset of the audit, the audit team expected to find that roles and responsibilities, key deliverables, training requirements and performance and reporting measures were clearly defined in an integrated framework supporting the overall management of information at Veterans Affairs Canada. Defined roles and responsibilities provide clarity, alignment, and expectations to those executing the work of appropriately managing departmental information.

Given that information management is a responsibility of all departmental employees, it further shows that it is critically important that all employees understand their roles and responsibilities and not just those who work in the Privacy and Information Management Division. If important departmental information is not maintained and easily accessible, there is a risk that not all information will be available to support informed decision making.

What we found

VAC does not currently have a governance framework relating to information management. During the time period the audit covered, the Department did have the

⁴ Internal Audit Sector of the Office of the Comptroller General: Core Management Controls, A Guide for Internal Auditors (2007).

2019-22 VAC Information and Data Strategy in place. This strategy was intended to ensure that the Department could make evidence-informed decisions based on reliable, accurate and quality data and analysis. Although this strategy was not specific to information management, it did include comments on governance frameworks and tools related to managing information.

As a follow-up to the implementation of this strategy, the audit team found a recent review of progress related to the strategy indicated that less progress was made than anticipated and that minimal information governance models and methodologies are in place at VAC. In addition, the review found that the initial state with respect to information governance may have been over-estimated and that information governance did not receive the attention it needed during 2019-22.

The team found that the Department has established an Executive Data Stewards Committee and a Data Stewards Committee. Terms of reference, meeting agendas and records of decisions are available. The documents do contain guidance on roles and responsibilities for chairs and members however, the focus is more on data than information management.

Interviews with staff within the Privacy and Information Management Division indicated that they were aware of their roles and responsibilities with respect to information management. As part of the audit, the Audit team conducted a survey of all VAC employees to gauge their level of knowledge related to information management and individual roles and responsibilities within the Department. 833 responses were received to the survey⁵:

- 67% of responses reported a Good or Very Good knowledge and understanding of their information management roles and responsibilities.
- 57% reported that information management was a priority for them.
- 63% reported that information management was a priority for their division.
- 63% reported that information management practices were either Good or Very Good within their division.

In August 2020, a presentation was made to Senior Management on the importance of recording and saving decisions resulting in any program changes related to the COVID-19 pandemic. A template for recording decisions was developed but it was never completed. Interviews with staff indicated that the document would be updated and available in June 2022. Having a formal governance framework with clear roles and responsibilities and regular reporting may have contributed to this document being completed in a timely manner.

⁵ The survey was sent to 3,455 employees resulting in a response rate of approximately 24.1%. Although results can vary greatly, a typical response to a public opinion research survey such as this is between 10%-20% so the Audit Team was very pleased with this response rate. However, it is important to note that the responses were self-reported, and the audit team was unable to confirm the quality of information management practices within divisions in addition to the actual knowledge level of employees.

3.1.2 Monitoring and reporting

Why it is important

Effective risk management and planning are supported by quality monitoring and reporting tools and processes. Monitoring is the process of systematically tracking key indicators to assess progress made in achieving goals and objectives. Ongoing monitoring also assists with informed decision-making and risk management.

The [Treasury Board's Policy on Service and Digital](#) explains how Government of Canada organizations manage service delivery, information and data, information technology, and cyber security in the digital era. Under this policy, there are requirements for establishing governance as well as planning and reporting to meet overall objectives and results including integrated decision making, improved government operations and an improved client experience.

What we found

VAC does not have formalized indicators to measure information management performance. Interviews with staff indicated that a new reporting position had been created within the past year, however, the primary focus of the position was related to Access to Information and Privacy requests at the outset with the future goal of adding information management related reporting.

As part of Treasury Board of Canada's Management Accountability Framework reporting, VAC is required to respond to several questions on various topics. For the 2021-22 reporting cycle, there was only one question related to Information Management regarding the management of information throughout its lifecycle across multiple systems. In this regard, the Department has significant work ahead to ensure information and data is managed across its various systems throughout its life cycle.

The Privacy and Information Management Directorate has a Privacy Impact Assessment Needs Determination process in place to review upcoming work activities to ensure privacy and information management requirements are identified, analyzed and an important part of project planning. The process requires completion of a document explaining all the details of the work activity and how information will be managed during and after the work activity.

As part of this process, advice and recommendations are received from the Privacy and Information Management team as well as the IT Security team and a final document is signed by all parties involved. Approximately 60 documents have been completed since the beginning of the audit period, however, due to lack of resources and prioritization activities, no follow-up has been completed to ensure compliance with the recommendations.

The audit team also noted that more detailed reporting is expected to be available in future regarding information management as part of regular reporting against the *Policy*

on Service and Digital. This reporting is expected to assess the Department's current capability with respect to governance, information and data discovery, access, sharing, reuse as well as retention and disposition.

Interviews with four other federal departments revealed that limited performance measurement and monitoring of information management is not unique to VAC. However, one department took the available measures further by developing and adopting several performance indicators with accompanying measures to better assess their progress on their goals and objectives related to information management.

3.1.3 Training and available resources for staff

Why it is important

Having relevant training and resources available to support staff with information management activities is critical to ensure the overall success of managing information at VAC. Offering effective training and resources creates a learning environment that encourages growth and development.

What we found

There are numerous policies, procedures, business processes, training materials relating to information management available for staff through the Information Management page on the VAC at Work intranet site. However, 45% of survey respondents indicated that they did not know or were unsure where to find information related to information management policies, procedures and guidance.

The Privacy and Information Management Directorate provides Information Management 101 training for new employees, however it is not mandatory:

- Provided to 361 participants in fiscal year 2020-21 (of 757 new hires)
- Provided to 73 participants in fiscal year 2021-22 (of 351 new hires)

In addition to training on IM best practices, training related to GCdocs is also available on the intranet site. GCdocs specific training has evolved over the years. With the initial implementation of GCdocs in 2012-13, a two-day course was provided by the Information Management staff which included user training on the GCdocs system as well as best practices for information management. More recently, the training was condensed to 2 hours with major focus on tip and tricks for using the system.

Interviews also indicated that information management training is available on the Canada School of Public Service website, however, currently no training related to information management is mandatory for VAC employees. Additionally, staff raised the suggestion of introducing information management champions throughout the Department to raise awareness and help support new and experienced employees with their information management needs. The audit team found that another Department

has used a similar initiative and reported positive feedback.

3.1.4 Recordkeeping tools

Why it is important

Ensuring information is appropriately maintained and stored allows for good governance, informed decision making and the efficient and effective sharing of public information. Equipping employees with the appropriate tools and resources to carry out their information management responsibilities is equally as important to meet this goal.

Management of information throughout its life cycle to disposition ensures that proper information is safeguarded, maintained and available when it's needed.

What we found

GCdocs has been the official corporate repository at VAC since 2012-13. This has led to the gradual reduction in use of other methods for saving documents such as the reduction in use of shared drives. However, employees who responded to the information survey, reported saving documents using various methods such as:

- GCdocs
- Shared Drives
- Desktop
- Personal drive
- MS Teams

In terms of comfortability with using the tools currently available for recordkeeping:

- 51% indicated they were comfortable
- 30% were somewhat comfortable with using the available tools
- 19% were somewhat uncomfortable or not comfortable

The audit team also found that although the Department has interim methods for storing secret documents, there is no consistent or approved method. A solution was identified, and implementation began prior to the COVID-19 pandemic, however the pandemic put implementation on hold, and it has not been completed.

Interviews with Information Management and Information Technology staff indicated that the full functionality of GCdocs has not been implemented. Further functionality was to be implemented later as a part of subsequent phases of the project, however, these were not implemented due to other competing priorities at the time. The lack of full implementation of GCdocs functionality has resulted in challenges ensuring that correct information is stored, and it is likely that GCdocs currently contains a large amount of transitory information.

Interviews with staff suggested that VAC may be moving toward a replacement for GCdocs. The audit team interviewed representatives from other Departments and found that some use GCdocs only while others use a combination of GCdocs with other collaboration tools.

3.2 Audit conclusions

VAC has created an Executive Data Stewards Committee which is important in governing data and information at the Department. However, the lack of an effective and formal governance framework results in a lack of oversight of information management initiatives, projects, and risks.

Basic monitoring and reporting of information management is in place, but the lack of a formalized process with identified indicators makes it difficult to accurately measure overall performance.

The Department has some information management training available, however, it does not appear to be standardized or consistent for employees with no mandatory training in place.

VAC has adopted GCdocs as its official repository for supporting recordkeeping requirements. However, without a consistent and approved method to store secret files and retention/disposition scheduling, it risks making secret information accessible and holding too much transitory information. Furthermore, the possible replacement of the existing system for saving information may result in some similar challenges if it does not fully meet information management retention and disposition requirements.

3.3 Audit recommendations

Recommendation 1

It is recommended that the Assistant Deputy Minister, Chief Financial Officer and Corporate Services develop an official governance framework for information management including, but not limited to:

- Roles and Responsibilities
- Training and Awareness
- Performance Measurement and Monitoring

Management agrees with this recommendation.

The Privacy and Information Management Directorate (PIM) will develop an Information Governance Framework. The Framework will integrate with the VAC *Information and Data Strategy 2022-28*, and the renewed Federal Data Strategy

Roadmap. Components of this Framework will address the three pillars outlined in this recommendation across the domains of privacy, records management, data governance, litigation readiness, analytics, risk and compliance, and security. Addressing these pillars will ensure VAC meets its obligations.

Pillar I: roles and responsibilities will lay out how each employee's role fits within the overall Information Governance hierarchy and address each person's responsibilities (e.g. recording decisions, version control, retention rules, disposition authority)

Pillar II: training and awareness will describe the tools required to support employees in meeting their roles and responsibilities (e.g. mandatory and/or suggested training sessions, guidance documents, business processes)

Pillar III: performance measurement and monitoring will allow us to monitor overall risk by establishing and reporting on key performance indicators while also identifying and addressing information management gaps across the Department. More specifically, this will assess:

1. How well VAC is managing its records through tangible indicators (e.g., proper disposition of records having met their retention, version control, proper use of personal spaces, volume of records)
2. The level of compliance with legislated and policy requirements - are corporate and program areas following functional direction and advice and guidance provided (e.g., PIAND recommendations, contract compliance) – and associated level of risk
3. Gaps in knowledge which require additional support through development of training material and/or guidance material for the Department.

Target date: December 2023

Recommendation 2

It is recommended that the Assistant Deputy Minister, Chief Financial Officer and Corporate Services implement an enhanced, efficient and effective solution to better safeguard departmental corporate secret documents.

Management agrees with this recommendation.

Before the advent of Government of Canada Secure Infrastructure (GCSI), VAC did not have a specialized repository for documents classified above Protected B. To facilitate ease of movement and collaboration on SECRET documents a shared drive with restricted access, called the "Drop-off Area" (DOA), was established as a temporary area for the organization.

VAC began implementation of GCSI but had not fully implemented it prior to the pandemic. The future of GCSI is still under examination by the GOC and there is

currently no option to use GCSI outside of the physical office environment.

In order to reduce the risk associated with the DOA the IT/IM/Security teams have been working on the implementation of “SDocs”, a new folder structure presented on Citrix. The objective of SDocs would be to provide enhanced security from the current DOA, increased flexibility to users, and allow us to clean up the current access, permissions, and uses of the DOA. This will replace the DOA as a collaboration and transitory space until such time as the GOC develops a SECRET solution (GCSI or something else) that will better meet both security and user/departmental needs.

Target date: March 2023

Recommendation 3

It is recommended that the Assistant Deputy Minister, Chief Financial Officer and Corporate Services implement a process to ensure that its systems, including any new systems, follow GOC standards for information management.

Management agrees with this recommendation.

Changes to the *Policy on Service and Digital* governing IM, as well as other related areas, were introduced on 1 April 2022. TBS is developing and testing a framework that VAC will use to assess the level of effort required to bring systems into compliance and quantify the risk level if compliance cannot be reached.

At this point, we are not able to confirm that the end state as described is attainable. Based on an initial review of the renewed policy suite, the effort to become fully compliant will be significant, and at some point may not be feasible from a financial, capacity and cost benefit perspective. Therefore, we may need to tolerate some risk of non-compliance, focusing on key areas for improvement.

Once released, VAC will implement a process to apply the framework to our systems, outline the risks and costs associated with meeting the policy requirements, and ensure when value-added or feasible, existing and future systems will follow the standards for Government of Canada Information Management.

Target date: May 2024

4.0 Audit opinion

Based on the findings above, the audit team determined that the management of corporate information at VAC requires improvement. Although some of the tasks were informally carried out, improvements including a formal governance framework, a solution for secret documents and ensuring the Department is well positioned to meet

the changes recently implemented in relation to the Government of Canada *Policy on Service and Digital*, will help the Department better manage its information going forward.

Appendix A - audit criteria

Objective	Criteria
<p>1. Provide reasonable assurance that VAC has implemented an effective management control framework which includes accountability, roles, responsibilities and monitoring to mitigate information management risks</p>	<p>A. The Department has implemented an effective governance framework and has bodies in place to ensure sufficient oversight of Information Management risks and initiatives.</p> <p>B. The Department has clearly defined and communicated roles and responsibilities relating to Information Management.</p> <p>C. The Department has a performance monitoring and reporting process in place to evaluate and report on Information Management activities.</p>
<p>2. Provide reasonable assurance that VAC has implemented effective operational and technical controls through the organization which includes recordkeeping methodologies and tools as well as awareness and training activities to mitigate risks related to Information Management.</p>	<p>A. Department provides employees with the necessary training, tools, resources and information to support them in discharging their Information Management responsibilities.</p> <p>B. The Department has the appropriate tools and processes in place to support recordkeeping requirements throughout the information life cycle.</p>

* The audit team confirmed that all of the above criteria were met unless otherwise stated in this audit report.

Appendix B - methodology

Methodology	Purpose
Interviews	Interviews with VAC staff including staff whose responsibilities are not specifically IM related as well as senior management to assess governance and controls, assess compliance with relevant policies and processes and to gauge the level of knowledge and understanding of IM roles and responsibilities and to identify any gaps.
Documentation Review	Documentation reviews were completed to determine whether VAC employees have access to the appropriate tools and training (guidance, tools, and procedures) for discharging their roles and responsibilities related to IM.
Survey	A survey was conducted electronically to complement interviews and assist in determining information management knowledge and practices within the Department.
Data Analyses	Reviewed and analyzed any data that exists related to information management to determine if the Department is meeting its requirements for IM and to see if any gaps exist in available data.