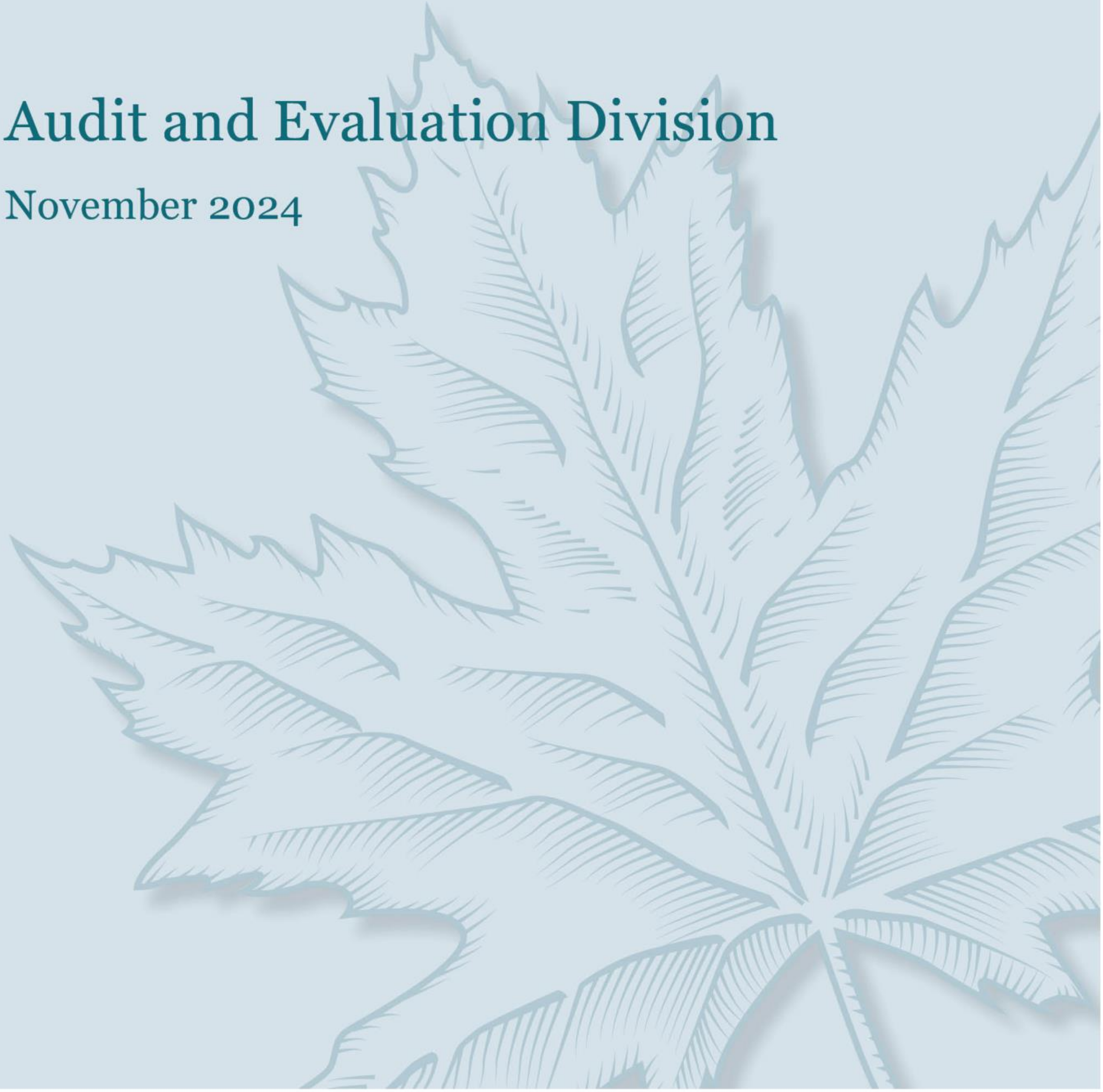
Veterans Affairs Canada Anciens Combattants Canada

Canada

Audit of Systems Access Control

Audit and Evaluation Division

November 2024



ISBN 978-0-660-77359-9

Acknowledgements

The audit team gratefully acknowledges Veterans Affairs Canada staff in Information Technology, Information Management, Administration and Privacy Division, as well as staff from Service Delivery and Program Management. Their contributions were essential to the success of this audit.

Table of Contents

Executive summary

Background

Veterans Affairs Canada (VAC) has a responsibility to protect the sensitive client information it holds. This audit set out to ensure systems and controls are designed to ensure the appropriate people are accessing information in certain systems (CSDN and GCCase-PFL) in the appropriate manner. The scope period was between 1 January 2023 and 31 December 2023.

Key findings and conclusion

We found that requirements and procedures are in place, however there is room for improvement. Access privileges are defined using access matrices, which map the relationship between roles and the permissions or access levels granted to them, but responsibilities for the matrices are unclear. Changes are needed in internal controls for system administrator accounts in PFL.

Users receive training and regular reminders about acceptable use of the systems, however there is no acceptable use communication at the time access is granted. There is no periodic review of access privileges, nor any regular monitoring of user activities, although the systems do track some user activities.

Overall, the audit team determined that these internal controls require improvement. We did not find any evidence of privacy breaches, as that was not the focus of the audit. However, if the weaknesses identified are not addressed, the potential for privacy breaches puts VAC at a reputational risk. Clients may lose trust in VAC's ability to hold and manage their private information.

Highlights of recommendations

The audit identified recommendations to:

- Update and approve procedural documents
- Define and communicate responsibilities for access matrices
- Improve internal controls for system administrator access in PFL
- Inform authorized users of acceptable use at the time access is granted
- Perform periodic review of user accounts and monitoring of user activity.

Chief Audit Executive's Signature

Lindy McQuillan, CPA, CMA
Chief Audit Executive
Veterans Affairs Canada

1.0 Background

VAC has multiple information systems that hold personal and sensitive information for approximately 180,000 clients. Staff, contractors and other users require access to this information to provide services to Veterans and their families. VAC has a responsibility to protect this information from unauthorized access. Systems and controls must be designed to ensure the appropriate people are accessing the information systems in the appropriate manner.

Two of the widely used information systems that hold VAC client information are the Client Service Delivery Network (CSDN) and GCcase- PFL[1] (PFL). Access to these systems is granted by Access Control Officers (ACO) in the IT Operations directorate. To be granted access, a user submits a request (using the program AssystNet), detailing what access (role/work description) is needed, and includes evidence of their supervisor's approval. This evidence is normally an email, although there are some other methods, such as the supervisor being the person to submit the AssystNet log. The ACO reviews the request, communicates with the user if required information is missing, and verifies the roles/work descriptions to the appropriate matrix. Once all required information has been submitted, the ACO grants the access to the system(s) and roles/work descriptions requested, using CSDN System User Access Tool (for CSDN) or Dynamics 365 (PFL).

An email is sent to the user confirming that their access has been granted. Users are then only able to see and/or edit the information contained in the user roles/work descriptions assigned to them.

Removing a user's access is done in a few ways. For CSDN, if an end date for the user's access is known, it is entered upon setting up the access, and access is automatically removed at the end date. There is no similar option in PFL. When access is to be changed or removed for either system, a request is submitted (by the user or their manager) detailing the changes to be made. The request is submitted using the program AssystNet for a user leaving the department and requesting removal of all access, and using an email template for a user moving within the department and requesting a change in access. The access control officer reviews the request and communicates with the requestor if any information is missing. Once all required information has been submitted, the ACO changes or removes access using the same programs for granting access.

[1] GCcase - PFL was the application used at the time of the audit. After the audit scope period, the PFL application was migrated to the cloud and is now referred to by staff in IT Operations as PFL, which will be used throughout the audit report. Although the process for access control officers changed slightly with the migration, the findings of this report are all still applicable.

2.0 Audit results

As a preamble to the audit results, the audit team wants to note that while the audit scope was CSDN and PFL, we heard from staff members that some of the issues identified in the following sections are not only related to CSDN and PFL, and some of the issues are easier to address at the system design phase. Thus, we would encourage VAC management to use this audit’s findings and recommendations to help reduce the risks in other existing information systems, as well as in the development and enhancement of new and legacy systems (for example, with the ongoing IT Modernization project).

2.1 Requirements and procedures

Requirements and procedures are in place, however gaps were identified, and inconsistent documentation for the approval of access requests is an issue.

Why it’s important

Requirements and procedures are important internal controls because they set clear rules on how to maintain the security and privacy of critical information. They also help VAC employees know what is expected of them, which reduces mistakes and confusion. Overall, they help create a consistent and efficient workplace.

What we found

Access Control requirements are generally set through VAC’s Security Standards for Access Control (referred from this point on as the Standards). However, the Standards were produced in 2013 and include some outdated information.

VAC has established procedures for the creation, modification, and disabling of accounts for CSDN and PFL, but some are outdated and/or need approval. Gaps in the procedures provided have been identified. For modification and disabling of accounts, weaknesses have been identified in the ability to ensure Access Management[2] is notified when an employee changes roles or leaves the Department.

Procedures are not established for the periodic review of accounts for CSDN and PFL, and there is no documented process in place for setting up system administrator [3] access in the production environment for PFL.

On a positive note, there are a large volume of procedures Access Management has prepared. Although some are dated and need updating, there were many different

[2] Access Management is the team within the Information Technology, Information Management, Administration and Privacy Division that provides access, administration, and control for most of the Information Technology systems and applications approved for VAC.

[3] System administrators typically have significantly more access to systems than an average user, as they perform behind the scenes work such as programming, assigning access, etc.

folders within GCdocs that seemed well organized with all kinds of procedures for different scenarios.

To test existing internal controls, a sample of 172 new CSDN accesses/requests and 185 new PFL accesses/requests were tested. Our audit testing attempted to determine whether:

- Proper approvals were in place for access to be granted, and
- Proper access was granted as per the request.

For CSDN, we found that:

- 87 accesses (50%) clearly had approvals attached to the log (i.e. request). Of those that did not clearly have approvals, 37 accesses (22%) were employees of a contractor that follows different procedures that do not result in a clear audit trail of approval, 9 access requests (5%) were later cancelled, and 39 accesses (23%) appeared to have approval but the evidence in the file wasn't clear (for example, the request was not specific enough);
- 115 accesses (67%) clearly had appropriate roles assigned as per the logs. Of the remaining sample items,14 (8%) had roles assigned that did not match the logs, 9 (5%) had the request later cancelled, and 34 (20%) appear to have appropriate roles assigned but the evidence was not clear (e.g., access request based on mirroring another user)

For PFL, we found:

- 90 accesses (49%) clearly had approvals attached to the log. Of those that did not clearly have approvals, 5 accesses (3%) did not have appropriate approval, 77 accesses (41%) appeared to have supervisor approval but the evidence wasn't clear (for example, the request was not specific enough), and for 13 sample items (7%), the audit could not find evidence to conclude, either due to the way access was assigned or due to data limitations (See Appendix A).
- 150 accesses (81%) clearly had appropriate roles assigned as per the logs. Of the remaining sample items, 14 (7%) had roles assigned that did not match the logs, 3 (2%) appeared to have appropriate roles assigned but the evidence wasn't clear (e.g. roles requested were not specific enough to match the matrix), and for 18 items (10%), the audit could not find evidence to conclude, either due to the way access was assigned or due to data limitations (See Appendix A).

More broadly, we found inconsistencies in documentation obtained for the approval of access requests, making it difficult to conclude if proper approvals were in place and if Access Management granted the proper access.

What is the effect / impact?

There is a risk of access decisions being made that do not align with management's expectations due to gaps identified in both the requirements and procedural documents. In addition, VAC is at a greater risk of staff inappropriately accessing sensitive Veteran information because of errors related to approvals and providing access. VAC is also at risk of employees of a contractor inappropriately accessing sensitive Veteran information due to a weak approval process.

Recommendation 1

The Director General, Information Technology, Information Management, Administration and Privacy Division should update the documentation defining access control requirements along with procedural documents for creation, modification and disabling of access to CSDN and PFL for both internal and external users.

Management response

Management agrees with this recommendation. We will revise and enhance our requirement and procedural documentation to include clear processes for the creation, modification, and disabling of access for both CSDN and PFL.

This effort will involve collaboration with IT and business CSDN & PFL stakeholders to ensure documentation is aligned with organizational procedures and approval processes. These measures will address existing gaps in current procedures and documentation and reinforce a consistent and secure approach to access control management for CSDN and PFL.

Target completion date: December 2025

2.2 Defining access privileges

Access privileges are defined using access matrices.

Responsibilities to ensure matrices apply the principles of least privilege and segregation of duties are unclear.

There is a weakness in internal controls for system administrator accounts in PFL.

Why it’s important

Defining access requirements based on the principles of least privilege and segregation of duties is important for protecting sensitive information. The principle of least privilege means that individuals should only have access to the resources they need to do their jobs, reducing the risk of accidental or malicious misuse. Segregation of duties ensures that no single person has control over all aspects of a critical process, which helps prevent fraud and errors. Together, these principles create a safer environment by minimizing the chances of unauthorized access and promoting accountability.

We expected to see that VAC had put requirements in place to implement these principles when determining access privileges in CSDN and PFL and that the requirements were implemented.

What we found

VAC’s Security Standards for Access Control indicate that all systems must establish a division of responsibilities and separate duties for individuals as necessary, to eliminate conflicts of interest. It also indicates that systems and applications must employ the concept of least privilege, limiting authorized access for users as necessary, to accomplish assigned tasks. The audit team tried to determine whether these requirements were met using the matrices for each system that define access privileges to be assigned to users.

CSDN and PFL each have a matrix that was designed to organize and manage who can be assigned what access in each system. The systems are designed to enforce the access definitions in the matrices, and Access Management uses the matrices to assign access to users.

Facts from our review of each matrix can be found below, with overall conclusions, impacts and recommendations at the end.

CSDN

Matrix

The CSDN Matrix is a complex document over fifty pages long, providing work descriptions and multiple levels of access for each work description.

There is a related list of functional authorities, which is a document that identifies people to be consulted if any changes are to be made to the matrix. The functional authority list is based on name, rather than position. This makes it hard to ensure the list is kept up to date, as people regularly change positions within the organization. Based on discussions with a some of the functional authorities, they are not provided training as to what responsibilities are held as a functional authority, and minimal guidance is available. Thus, they may not be aware of their requirements to consider least privilege and segregation of duties if they are approving changes to the matrix.

Access Management claims administrative responsibility for the matrix, however, we were unable to determine who has overall responsibility for the content of the matrix. The functional authorities list is a 19-page document of names responsible for individual access levels and does not assign overall responsibility. Thus, it is difficult for VAC to ensure the matrix accurately addresses the risks to the organization regarding least privilege, segregation of duties, and inappropriate access to information.

On a positive note, there is specific and clear guidance on how to make changes to the matrix, which includes an approval process by functional authorities, with a documented trail of requested changes and approvals. In addition, the matrix and functional authority list are available in both official languages and clearly document who is responsible for the different types of access in CSDN.

Least privilege

Multiple interviews with employees referred to assigning individuals the least amount of access possible to do their work, that CSDN is very stringently controlled, and access is provided on a screen-by-screen basis. This is evidenced by the matrix itself, which is over 50 pages long, and provides work descriptions and multiple levels within each work description. When access is granted, the user gets access to all clients in the system.

PFL

Matrix

The PFL System Access Matrix is an approximately two page excel document which is relatively simple and lists business groups and the roles provided to each business group.

Any changes are discussed with the product owner and others as necessary. However, there is no listing of people to be consulted for changes or guidance on who to contact. This makes it hard to know who has the knowledge and/or authority to make changes.

There are no documented processes for how to make changes to the matrix, but changes are tracked in a log with an audit trail.

Access Management claims administrative responsibility for the matrix, however the audit team was unable to determine who has overall responsibility for the content of the matrix. It is therefore difficult for VAC to ensure the matrix accurately addresses the risks to the organization regarding least privilege, segregation of duties, and inappropriate access to information.

On a positive note, the matrix is available in both official languages and clearly documents what access in PFL each business group gets.

The audit team found examples of changes to the matrix without formal documented approval, changes that did not get reflected in a timely manner, and areas of the matrix that appeared to need updating.

Least privilege

Multiple interviews referred to PFL having fairly open access, with the system relying on employees' own awareness about what information is appropriate to access in the course of their jobs. With that being said, the matrix does clearly define business groups and their access roles. We were informed that once a role is provided, users get access to the whole application, or multiple areas within the application, for that role. However, users need to be part of a team to have work assigned to them. When access is granted, the user gets access to all clients in the system.

System administrator privileges

The system administrator role could not be found on the matrix, and Access Management does not set up these accounts under their normal business processes. We were informed that access is granted by IT staff.

As of 30 June 2023, there were 63 user IDs in PFL with active system administrator roles assigned to them. The common positions associated with the individuals' names attached to these roles were staff who work in Veteran Client Applications (i.e., most likely developers); Staff who work in Access Management (who assign access to other users); and Business Analysts. There were at least 6 individuals with more than one username that has system administrator access. Most user IDs for Access Management also have the role Access Management Service Admin, but staff from IT Application Management informed us the role was never configured for accessing PFL specific records. The audit team was informed that the system administrators have full access to client data and can make changes to the system in the production environment.

PFL
The audit team was informed that following the conclusion of the audit, system administrator access was cleaned up. The team obtained data as of 1 December 2024, identified 28 user IDs with system administrator access in PFL, which appears more reasonable.

For both CSDN and PFL, we were able to find some evidence that segregation of duties was considered when the matrices were created (i.e. when access privileges were defined). This included a PFL checklist and some notes on the PFL matrix identifying some roles to be segregated. For CSDN, numerous interviewees confirmed that CSDN was stringently controlled, and we obtained some instructions for functional authorities that referred to consideration of segregation of duties when approving changes to the CSDN matrix. However, we were unable to find a clear definition or analysis of what VAC defined as duties that should be segregated within each system to test that they were properly segregated. As an example, some employees raised concerns about Additional Pain and Suffering Compensation (APSC) staff both processing and paying decisions, but it was unclear whether VAC had undertaken an analysis of whether this was truly an issue with segregation of duties.

As outlined in the details above, the two matrices are quite different in both their set up and in the processes to make changes. This can be expected, as they are two different systems that have different roles to play and were implemented at different times. The audit did not attempt to evaluate whether one defined access privileges better than the other. However, without the ability to determine who was responsible for each matrix, the audit team could not gather information on VAC’s risk tolerance when it comes to the matrices’ role in protecting access to sensitive client information. It would appear as though the set up of the PFL matrix accepted a higher level of risk than the CSDN matrix, and VAC should evaluate whether that falls within their acceptable level of risk.

What is the effect / impact?

Each system included in the scope of the audit houses similar, sensitive client information. Yet, access privileges have been defined very differently. There is a risk that one system or the other does not meet the risk tolerance thresholds of the Department. Since there has been no assignment of responsibility for the matrices, there is a greater risk of inappropriate or unauthorized changes to the matrices that have not considered the required concepts of least privilege or segregation of duties.

Poor controls around system administrator access in PFL poses both a cyber security and insider threat. Cybercriminals are aware that system administrator roles have even more access than the average user, so are a prime target. Inside the organization, there is a risk that system administrators may abuse their powers.

Recommendation 2

The Director General, Service Delivery and Program Management, in collaboration with the Director General, Information Technology, Information Management, Administration and Privacy Division should define and communicate who is responsible for access control matrices for CSDN and PFL and what is involved with those responsibilities.

Management response

Management agrees with this recommendation. VAC has established roles and responsibilities for Client facing systems such as CSDN and GC Case (PFL). We will leverage these existing responsibilities to ensure assignment of responsibility for the matrices. VAC will ensure clarification and communication of the specific duties occur across stakeholders and partners.

Target completion date: March 2026

Recommendation 3

The Director General, Information Technology, Information Management, Administration and Privacy, should develop and implement a process for assigning system administrator access in PFL and review current users with system administrator access, remove unnecessary users of this role, and add the role to the matrix.

Management response

Management agrees with this recommendation. We will implement a process to request, approve, and assign elevated privileges in PFL and ensure all parties involved are aware. We will perform a review of current users with System Administrator access and remove users that no longer require this role if any. We will add the System Administrator role to the access control matrix.

Target completion date: June 2025

2.3 Acceptable use

Users receive training and regular reminders about acceptable use. However, at the point of becoming an authorized user of these two systems, there is no communication regarding acceptable use specific to the access they have just obtained.

Why it’s important

It's important to inform authorized users about the acceptable use of Government information systems to ensure that electronic client data is protected and used responsibly. By clearly outlining what is and isn’t allowed, we help prevent accidental or intentional misuse of sensitive information. This includes protecting client privacy, maintaining security, and following legal and ethical guidelines. When users understand these rules, it reduces the risk of data breaches, unauthorized access, or other mistakes that may harm clients or the Government. Proper training and communication help ensure everyone knows their role in safeguarding the information they work with.

What we found

New staff are provided information and training when they join the Department. Subsequently there is little follow up/refresher training provided unless an employee needs to do the initial security training for a second time (for example, if their security pass is expiring). Additional security and awareness training is being tracked and reported on as part of the Departmental Security Plan implementation (mostly for those getting new or updated ID cards).

Contract review was considered out of scope for the audit, however we did inquire as to whether the most sizable, non-government external[4] users of CSDN receive information on the acceptable use of government information systems to access electronic client data. We were informed that the external company has a mandatory training program on security awareness and privacy, operate under a corporate security policy, and that their standard operating procedures address the security requirements of the contract.

Within VAC, every 120 days, users must agree to an acceptable use pop-up message, which includes a reminder that employees must only access confidential or personal information if they have a genuine need to know to preform their duties, and this acceptance is tracked in a log. VAC hosts an annual Security Awareness and Right to Know week which provides further reminders to staff about not accessing systems containing personal information without a need-to-know, and has provided reminders in Friday Highlights and other email messages that go out to staff.

However, at the point of being granted system access, Access Management does not communicate to ensure the user understands their responsibilities as it relates to accessing client information.

What is the effect / impact?

Reliance on onboarding and subsequent general reminders leads to a risk that users accessing sensitive client data aren’t giving the information they are gaining access to the consideration it deserves. There is a risk that during employee onboarding staff may have ‘information overload’ that they cannot tie significance of sensitive client data directly to their work. If the email they receive when access is granted highlighted the importance, they may be able to better relate to it and thus remember to only access sensitive client data on a need-to-know basis.

[4] External users would include hired contractors and other non-VAC parties who need access to the information systems to fulfil the requirements of their contract or agreement.

Recommendation 4

The Director General, Information Technology, Information Management, Administration and Privacy, should implement a process for informing authorized users about acceptable use of CSDN and PFL at the time of granting and changing access to these systems.

Management response

Management agrees with this recommendation. To address this, we will include appropriate communication on acceptable use when access is granted or modified. These efforts will enhance user awareness, promote accountability, and mitigate risks associated with unacceptable use.

Target completion date: June 2025

2.4 Access review

VAC does not undertake periodic review of access privileges.

Why it's important

It's important to review access to IT systems regularly to ensure that only the right people have access to sensitive information. Over time, staff may change roles, leave the Department, or no longer need certain permissions. If access isn't updated or removed when it's no longer needed, it can create security risks. By periodically reviewing and adjusting access, VAC can reduce the risk of unauthorized access and ensure that sensitive information is only available to those who need it to do their job.

What we found

There are no procedures in place for Access Management to regularly review access to determine whether it should be removed. When Access Management grants CSDN access, there are processes in place to automatically terminate access on a specific date, but that capability does not exist in PFL.

VAC does not review access privileges periodically. They are instead reviewed as needed when issues arise. When this happens, consideration is given to whether it is a systemic issue by position, and action is taken as needed.

The audit team undertook data analysis and a judgemental sample to help conclude whether there are users that have access that should be removed. The findings are presented below. It should be noted that this was not a full review of all user access, nor a statistical sample.

CSDN	**PFL**
External	*External*
We were unable to test whether external users access to CSDN should have been removed due to the lack of controls in place. Staff suggested we reach out to the external users to confirm their continued employment. However, to reduce the risk of unauthorized access to CSDN, VAC should have this information internally, rather than relying on the external parties to notify them when to remove access.	We were unable to test whether external users access to PFL should have been removed due to the lack of controls in place. Staff suggested we reach out to the external users to confirm their continued employment. However, to reduce the risk of unauthorized access to PFL, VAC should have this information internally, rather than relying on the external parties to notify them when access is to be removed.
Internal	*Internal*
For other internal CSDN users, most of the forty-five sample items appeared to have access granted that was in accordance with their job title. We found evidence in three sample items that some access should have been removed. During the planning phase of the audit, we also identified two audit team members who had additional access that had not been removed from prior work. We also identified one audit interviewee who had access that should have been removed.	For other internal PFL users, we found evidence in two out of thirty sample items that some access should have been removed. During the planning phase of the audit, we also identified three audit team members who had additional access that had not been removed from earlier work. We also identified one audit interviewee who had access that should have been removed. We identified 78 access roles (52 individuals) that had email address with an @canada.ca ending rather than @veterans.gc.ca. We reviewed eight, and it would appear all were accounts where access should have been removed when the employee left VAC. It should be noted that in most cases, the user accounts were deleted, which reduces the risk of unauthorized access. Subsequent to the audit scope period, access was removed for all 78 user ID's that were identified.

What is the effect / impact?

Because the Security Standards for Access Control (the Standards) are outdated and there is no business processes in place for account reviews as required by the Standards, staff are less likely to prioritize the reviews and may perceive it to be of lesser importance. The staff responsible would not only have to do the account reviews, but also create the framework for account reviews, creating additional workload.

There is a risk that users access remains in place when it is no longer needed, giving users have access to information that they do not require to perform current duties. There is a greater risk of inappropriate access to sensitive client information.

Recommendation 5

The Director General, Information Technology, Information Management, Administration and Privacy should define, document, and implement a business process for periodic review of user accounts in CSDN and PFL.

Management response

Management agrees with this recommendation. To address this, we will implement a cyclical review process in which the responsible authorities for CSDN and PFL account access will periodically review and confirm that assigned access levels remain appropriate.

Target completion date: June 2026

2.5 Monitoring

VAC has not developed and implemented guidance for staff to monitor user activities in CSDN and PFL, nor are automatic reports generated. Monitoring occurs on an ad hoc basis as needed.

Why it’s important

Government of Canada mandatory procedures for IT Security Control dictate that Departments are to create, protect and retain information system audit logs and records to enable monitoring for each system, among other things. Active monitoring may detect both threats and events, reducing the risk of unauthorized access to sensitive client information. We expected to see that:

- CSDN and PFL were programmed to track user access and activity and generate regular reports,
- there were policies or business processes in place for audit log monitoring, and
- staff were regularly monitoring access in accordance with pre-defined requirements.

What we found

Based on our interviews, VAC has not prepared an audit log policy or business processes that would guide how to monitor user activities within the context of VAC’s risks and systems (CSDN and PFL for the purpose of this report). VAC system developers have configured CSDN and PFL to track which fields are being accessed by what users, enabling user activities to be monitored. However, the systems are not configured to generate automatic reports to be used for monitoring. Reports must be requested on a case-by-case basis.

After interviewing numerous individuals, there was no evidence of active monitoring of user activities in CSDN and PFL. Ad hoc reports are scripted or run on an as needed basis (for example, when there is a security event to be investigated).

What is the effect / impact?

Because there is no policy or business processes in place to require monitoring, staff are less likely to prioritize monitoring and may perceive it to be of lesser importance than other responsibilities. It is difficult for staff to monitor user access without reports that generate automatically. The staff responsible would not only have to do the monitoring, but also create the framework for monitoring, creating additional workload.

By not actively monitoring user activities in CSDN and PFL, there is a risk of inappropriate access to sensitive client information going undetected, leading to potential privacy breaches.

Recommendation 6

The Director General, Information Technology, Information Management, Administration and Privacy, should define, document, and implement a business process to enable monitoring, reporting, and analysis of user activities in CSDN and PFL.

Management response

Management agrees with this recommendation. A business process will be developed to routinely monitor access to sensitive information in CSDN and PFL. The process will include appropriate administrative investigation and follow-up when warranted. Training and awareness will also form part of the solution to reinforce the importance of need to know while enabling users to perform their duties effectively.

Target completion date: December 2025

2.6 Audit opinion

The audit opinion is provided based on the scope of the audit to ensure compliance with elements of the Government of Canada Directive on Security Management. The audit objectives relate to limiting user access to electronic client data and monitoring of user access. Two of VAC’s key information systems – PFL and CSDN –were included in the scope of the audit.

VAC has some internal controls to limit user access to electronic client data, however there are gaps in these controls. Requirements and procedures for granting, modifying and removing access to CSDN and PFL require improvement. There is a need to clarify responsibilities and improve processes to define access roles, including system administrators. Additionally, VAC is not undertaking periodic reviews of user access as required. When it comes to monitoring of user access, VAC has implemented some measures to enable user activities to be monitored, however there are gaps in these measures and no current monitoring is being done. Overall, the audit team determined that key internal controls reviewed require improvement.

In each section noted above, the impacts of the internal control weaknesses were identified. We did not find evidence of privacy breaches, as that was not the focus of the audit. However, if the weaknesses identified are not addressed, the potential for privacy breaches puts VAC at a reputational risk. Clients may lose trust in VAC's ability to hold and manage their private information.

The audit conforms with the Institute of Internal Auditor's International Standards for the Professional Practice of Internal Auditing, as supported by the results of the quality assurance and improvement program. The audit findings and conclusions contained in this report are based on sufficient and appropriate audit evidence gathered in accordance with these standards. 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.

Appendix A – About the audit

Scope and Objectives

The audit scope covered the internal controls in place between 1 January 2023 and 31 December 2023 to ensure compliance with elements of the Government of Canada Directive on Security Management relevant to the objectives stated. The audit team identified information systems that house client information that have access control risks to include in the audit. The audit included two of VAC's key information systems – PFL and CSDN. Although there is an IT modernization project currently in progress, it is a long-term project in which system access controls may have to be considered. Therefore, recommendations from this audit should still be able to add value to the department moving forward.

All other information systems were out of scope for the audit. The audit scope did not include security screening, security categorization and marking, physical security, cybersecurity, security assessment and authorization, password controls, or controls unique to access by Royal Canadian Legion.

The objective of the audit is to assess VAC's actions to protect electronic client information from unauthorized access by staff and other system users. The audit set out to answer the following questions:

Has VAC implemented internal controls to ensure that access to electronic client data is limited to authorized users who have a need for access?

Has VAC implemented internal controls to create information system audit logs and records to enable monitoring and reporting for each system?

Audit criteria

Objective 1

Has VAC implemented internal controls to ensure that access to electronic client data is limited to authorized users who have a need for access?

Criteria

a) VAC has established requirements and procedures for the creation, modification, periodic review and disabling of accounts providing access to electronic data
b) VAC defines access privileges based on departmental security requirements and the principles of least privilege[5] and segregation of duties
c) VAC informs authorized users about the acceptable use of government information systems to access electronic client data
d) VAC reviews access privileges periodically, and removes access when it is no longer required.

[5] Least privilege refers to allowing only authorized access for users which are necessary to accomplish assigned tasks.

Objective 2

Has VAC implemented internal controls to create information system audit logs and records to enable monitoring and reporting for each system?

Criteria

a) VAC has implemented measures to enable user activities to be monitored to ensure users are accountable for their access to electronic client data
b) VAC monitors the acceptable use of access to electronic data

Limitations

The audit was limited because we were unable to access the Dynamics 365 system needed for a complete review. The user roles Access Management was able to provide to the audit team would have given the auditors write access, which posed an unnecessary risk of the team making accidental changes in the system. Without access to this system, the team had to rely on data reports to assess certain areas. As a result, the audit evidence is less reliable for conclusions around the PFL new access test (Section 2.1) and PFL access removal test (Section 2.4).

There were data limitations with the population data used to pull samples of new users within the scope period for both systems. There were two datasets available, however, neither covered all risks that the audit team identified. Therefore, two sets of data were combined, duplicates were removed, and a sample chosen from the combined report. We were not able to verify the completeness or accuracy of the combined report.

For one data set in CSDN, we received 5 different versions during our audit. While it appeared that the final data was accurate and it was able to be used in testing, we were unable obtain absolute assurance regarding its accuracy.

The audit was subject to certain limitations due to the size and technical nature of the subject matter. Despite our best efforts, some aspects of the audit could not be fully tested and we relied on the opinions of multiple interviewees to confirm that certain things were happening in the information systems. In another case, we verified that reports existed using data, however, did not test for adequacy of the reports.

It is important to note that the above noted limitations may have impacted some of the findings of the audit, however, we did not identify any limitations that would impact the audit opinion or recommendations.

Methodology

Methodology	Purpose
Interviews	Inquired about processes in place for defining and implementing access requirements, communicating acceptable use of information systems to users, processes and frequency of reviewing access privileges, processes for identifying and implementing changes in access privileges due to movement or termination. Inquired about decision making processes and responsibilities for access control matrices. Inquired about processes in place for granting access to system administrator roles. Inquired about development of systems to enable monitoring of access, processes for and frequency of audit log monitoring.
Direct observation	Observed Access Management procedures to grant access to each system. Observed user logging into each system.
Documentation review	Reviewed process documentation to support the responses to interviews. Reviewed user access matrices in place to ensure consideration of least privilege and segregation of duties. Reviewed documents that VAC uses to inform authorized users about the acceptable use of government information systems to access electronic client data.
File review	Took a sample of new access granted to test whether procedural documents were followed and access was granted in accordance with approved access request. Took a sample of access in place at a particular time to determine whether access should have been removed.
Data analysis	Using list of current users for each system, performed data analysis on external (non-VAC) users and System Administrators.

Appendix B – Risk ranking of audit opinion

The following definitions are used to classify the ranking of the audit opinion presented in this report.

Well controlled

Only few, insignificant weaknesses relating to the control objectives or sound management of the audited activity are identified.

Generally acceptable

Identified weaknesses when taken individually or together are not significant or compensating mechanisms are in place. The control objectives or sound management of the audited activity are not compromised.

Requires improvement

Identified weaknesses, when taken individually or together, are significant and may compromise the control objectives or sound management of the audited activity.

Appendix C – Recommendations and management response

Audit recommendation	Management response	Timeline for completion
1. The Director General, Information Technology, Information Management, Administration and Privacy Division should update the documentation defining access control requirements, along with procedural documents for creation, modification and disabling of access to CSDN and PFL for both internal and external users.	Management agrees with this recommendation. We will revise and enhance our requirement and procedural documentation to include clear processes for the creation, modification, and disabling of access for both CSDN and PFL. This effort will involve collaboration with IT and business CSDN & PFL stakeholders to ensure documentation is aligned with organizational procedures and approval processes. These measures will address existing gaps in current procedures and documentation and reinforce a consistent and secure approach to access control management for CSDN and PFL.	December 2025
2. The Director General, Service Delivery and Program Management, in collaboration with the Director General, Information Technology, Information Management, Administration and Privacy Division should define and communicate who is responsible for access control matrices for CSDN and PFL and what is involved with those responsibilities.	Management agrees with this recommendation. VAC has established roles and responsibilities for client facing systems such as CSDN and GC Case (PFL). We will leverage these existing responsibilities to ensure assignment of responsibility for the matrices. VAC will ensure clarification and communication of the specific duties occur across stakeholders and partners.	March 2026
3. The Director General, Information Technology, Information Management, Administration and Privacy, should develop and implement a process for assigning system administrator access in PFL	Management agrees with this recommendation. We will implement a process to request, approve and assign elevated privileges in PFL and ensure all parties involved are aware. We will perform a review of current users with System Administrator access	June 2025

and review current users with system administrator access, remove unnecessary users of this role, and add the role to the matrix.	and remove users that no longer require this role if any. We will add the System Administrator role to the access control matrix.	
4. The Director General, Information Technology, Information Management, Administration and Privacy, should implement a process for informing authorized users about acceptable use of CSDN and PFL at the time of granting and changing access to these systems.	Management agrees with this recommendation. To address this, we will include appropriate communication on acceptable use when access is granted or modified. These efforts will enhance user awareness, promote accountability, and mitigate risks associated with unacceptable use.	June 2025
5. The Director General, Information Technology, Information Management, Administration and Privacy should define, document, and implement a business process for periodic review of user accounts in CSDN and PFL.	Management agrees with this recommendation. To address this, we will implement a cyclical review process in which the responsible authorities for CSDN and PFL accounts access will periodically review and confirm that access levels remain appropriate.	June 2026
6. The Director General, Information Technology, Information Management, Administration and Privacy, should define, document, and implement a business process to enable monitoring, reporting, and analysis of user activities in CSDN and PFL.	Management agrees with this recommendation. A business process will be developed to routinely monitor access to sensitive information in CSDN and PFL. The process will include appropriate administrative investigation and follow-up when warranted. Training and awareness will also form part of the solution to reinforce the importance of need to know while enabling users to perform their duties effectively.	December 2025

Appendix D – Glossary

Term	Definition
Business Group	The PFL matrix lists approximately 40 Business Groups that can be provided access to the system based on the type of work to be performed (e.g. BPO – CPC, Administrative Service Officer, Case Managers etc.). Each group receives between 1 – 5 PFL roles (security roles) that determine what records the system will provide them access to.
Client Service Delivery Network (CSDN)	The Client Service Delivery Network (CSDN) is an information system used by VAC staff to assist in the delivery of services to clients, including Veterans benefits and case management.
GCcase- PFL (PFL)	An information system used by VAC staff to assist in the delivery of the Pension for Life benefits (PFL) to clients who are living with a disability due to a service-related injury and/or illness.
IT Modernization Project	A VAC project that intends to simplify client service delivery systems to make them accessible, more user friendly, and easier to maintain.
Least privilege	The concept of limiting authorized access for users as necessary, to accomplish assigned tasks.
Legacy system	Outdated computing software and / or hardware that are still in use.
Matrix	A tool used to define and manage access rights to various systems, applications, or data. It outlines which roles have permission to access specific resources or perform certain actions within a system. It maps the relationship between roles and the permissions or access levels granted to them.
Risk tolerance	Risk tolerance is the willingness of an organization to accept or reject a given level of residual risk. Risk tolerance must be clearly understood by the individuals making risk-related decisions. Clarity on risk tolerance at all levels of the organization is necessary to support risk-informed decision-making and foster risk-informed approaches.

	Guide to Integrated Risk Management - Canada.ca
System administrator	Users who have significantly more access to systems than an average user, as they perform behind the scenes work such as programming, assigning access, etc.
Segregation of duties	The practice of dividing responsibilities for related tasks among different individuals to reduce the risk of errors, fraud, or inappropriate actions.
Work description	The CSDN matrix lists approximately 45 pages of Work Descriptions that can be provided access to the system based on the type of work to be performed (e.g. Disability Benefits Officer, Administrative Service Officer, Case Managers etc.). Each group receives numerous access levels (security roles) that determine what records the system will provide them access to.