August 2019

THE B.C. GOVERNMENT'S INTERNAL DIRECTORY ACCOUNT MANAGEMENT

An independent audit report

www.bcauditor.com

OFFICE OF THE
Auditor General
of British Columbia

CONTENTS

The Office of the Auditor General of British Columbia would like to acknowledge with respect that we conduct our work on Coast Salish territories. Primarily, this is on the Lkwungen-speaking people's (Esquimalt and Songhees) traditional lands, now known as Victoria, and the W̱SÁNEĆ people's (Pauquachin, Tsartlip, Tsawout, Tseycum) traditional lands, now known as Saanich.

623 Fort Street
Victoria, British Columbia
Canada V8W 1G1
P: 250.419.6100
F: 250.387.1230
www.bcauditor.com

The Honourable Darryl Plecas
Speaker of the Legislative Assembly
Province of British Columbia
Parliament Buildings
Victoria, British Columbia
V8V 1X4

Dear Mr. Speaker:

I have the honour to transmit to the Speaker of the Legislative Assembly of British Columbia the report, *Audit of the B.C. Government's Internal Directory Account Management.*

We conducted this audit under the authority of section 11(8) of the *Auditor General Act* and in accordance with the standards for assurance engagements set out by the Chartered Professional Accountants of Canada (CPA) in the *CPA Canada Handbook*—Canadian Standard on Assurance Engagements (CSAE) 3001 and Value-for-Money Auditing in the Public Sector PS 5400.

Carol Bellringer, FCPA, FCA
Auditor General
Victoria, B.C.
August 2019

AUDITOR GENERAL'S COMMENTS

CAROL BELLRINGER, FCPA, FCA
Auditor General

TO PROVIDE SERVICES for the people of British Columbia, government collects and electronically stores large amounts of sensitive and personal information. To ensure that the only individuals who have access to sensitive information are the ones who need it, every government employee and contractor must have a unique username and password to log in to government systems. Government's internal directory account service (commonly known as IDIR), authenticates users' identity when they log in to these systems, to ensure their access is legitimate.

Controlling access to government systems is fundamental to ensuring that only authorized individuals can access government's online resources and information. This means that effective controls over the creation of new user accounts, modification of existing accounts due to role or employment status changes, and disabling and/or removing user accounts when they're no longer needed, is essential. Also, periodically reviewing and monitoring the status and activities of user accounts is important to ensure appropriate use of account privileges, and to detect suspicious account activities and take corrective measures.

The Office of the Chief Information Officer (OCIO) has overall responsibility for managing the IDIR service, and each ministry and government organization manages its own employees' and contractors' IDIR accounts.

From our audit of IDIR accounts management for 5 ministries, we found a lack of understanding regarding the role of the OCIO versus individual government organizations as to their respective responsibilities for maintaining the central records of accounts. The OCIO needs to remind ministries of their responsibilities as defined in the OCIO's information security standards.

AUDITOR GENERAL'S COMMENTS

We also found that some of the government organizations that we audited are not consistently following the OCIO's key controls for restricting unauthorized access. We weren't looking for improper use of accounts or security breaches that could result from improper accounts. But, there is a risk of unauthorized access to some government systems because the organizations weren't following the OCIO's key controls as stated in its security standards.

Some government employees have significant access to, and abilities within, government systems. For example, a system administrator often has the ability to create or alter IDIR accounts for their organization's users. We found that these employees' activities are not consistently reviewed to ensure appropriate use of their powerful accounts.

During our audit, we also noted that the number of active user accounts did not match the number of government employees, and these discrepancies grew over years. That said, there may be good reasons for the discrepancy. For instance, there are *non-human* accounts for systems, such as printers or servers, that allow the systems to talk to one another. As well, some employees have multiple responsibilities and therefore require multiple accounts. For instance, a system administrator may have access for regular duties under one account and a second account for when they need to perform a sensitive task.

Another challenge is that employee and account information is stored in two separate databases. The OCIO has responsibility for IDIR, but the BC Public Service Agency (PSA) holds and maintains the list of current government employees in the payroll databases. As such, one of our seven recommendations is that the OCIO and the PSA compare the two lists to ensure legitimacy of the IDIR accounts.

We are pleased that early in 2018, the OCIO began cleaning up dormant accounts. This was a good first step. We recommend that the OCIO expand the scope of its account clean-up to include such things as accounts with non-expiring passwords.

AUDITOR GENERAL'S COMMENTS

The IDIR service is the first defense against unauthorized access to government resources and all it takes is one poorly managed user account to compromise the government systems. A strong coordination and commitment to key controls and management of IDIR user accounts between the OCIO and across ministries is fundamental to access control.

I would like to thank the staff at the Ministries of Citizens' Services; Finance – including its related branches and agencies; Health; Attorney General; and Forests, Lands, Natural Resource Operations and Rural Development for their cooperation and assistance during our work on this report.

Carol Bellringer, FCPA, FCA
Auditor General
Victoria, B.C.
August 2019

REPORT HIGHLIGHTS

*****

Every govt employee has a **unique ID** to login to govt systems

Govt's internal directory (IDIR) **authenticates each user's login**

IDIR is **FIRST DEFENCE AGAINST** UNAUTHORIZED ACCESS to govt online systems

OCIO → **ADMINISTERS** → **IDIR SYSTEM**

MINISTRIES → **MANAGES** → **MINISTRY STAFFS' IDIR ACCOUNTS**

Some organizations NOT FOLLOWING **OCIO's security standards = risk of unauthorized access** to govt systems

2018:

OCIO STARTS IDENTIFYING AND REMOVING INACTIVE ACCOUNTS. Needs to continue and expand efforts

We **WEREN'T LOOKING** for incidents of unauthorized access to govt systems

OCIO should work with ministries to fully **implement key controls** as per **security standards**

SUMMARY OF RECOMMENDATIONS

WE RECOMMEND THAT THE OFFICE OF THE CHIEF INFORMATION OFFICER:

1 work with ministries to:

a) apply clear roles and responsibilities as defined for the IDIR user accounts provisioning processes

b) reconcile the Information Security Policy and Standards as they relate to the maintenance of a central record of access rights for IDIR users

2 work with non-compliant ministries to ensure they:

a) develop and document ministry specific procedures for setting up IDIR user accounts for new employees and contractors

b) establish a formal training and education program for those who are involved in the IDIR service

c) implement a process ensuring only properly authorized IDIR user accounts requests are acted upon

3 work with non-compliant ministries to ensure they develop and document ministry-specific procedures for establishing access permissions for authorized IDIR user accounts to access applications.

4 work with non-compliant ministries to ensure they develop and document ministry-specific procedures for the removal of IDIR user accounts of terminated employees and contractors.

SUMMARY OF RECOMMENDATIONS

WE RECOMMEND THAT THE OFFICE OF THE CHIEF INFORMATION OFFICER:

5 work with non-compliant ministries to ensure they establish processes for reviewing privileged IDIR account users' access rights and monitoring their activities to ensure they are appropriate and authorized.

6 work together with the BC Public Service Agency to compare the IDIR user employee profiles with the government employee payroll database and where discrepancies are identified make the appropriate corrections.

7 work with ministries to expand the scope of the monthly review of IDIR user accounts to include checking for non-expiring password settings and IDIR accounts that have remained active, even after employees and contractors no longer work for government.

RESPONSE FROM THE MINISTRY OF CITIZENS' SERVICES

The Province appreciates the careful analysis and dialogue on the Internal Directory Account Management report recently completed by the Office of the Auditor General (OAG). This report provides valuable feedback to inform ongoing government efforts to maintain the accuracy of its systems. I appreciate the OAG acknowledging the positive work we are doing and helping to validate government's current course of action to increase security in the area of access control.

The B.C. government takes the security of its systems seriously and accepts all seven recommendations in the report. While we do have security controls in place to protect internal directory accounts, there is more work to be done in this area.

The Office of the Chief Information Officer (OCIO) executed its plan to improve accuracy of internal directory accounts in January 2018 and, working with the ministries (Ministry of Citizens' Services, Ministry of Health, Ministry of Attorney General, Ministry of Finance and the Ministry of Forests, Lands, Natural Resource Operations and Rural Development), has made significant progress. The Province will continue these efforts and expand them going forward to ensure records for user accounts remain accurate. The OCIO will also work with the BC Public Service Agency (PSA) to ensure employee profiles in government's internal directory are consistent with the information maintained in the PSA's systems.

The information provided by the Internal Directory Account Management report provides valuable information regarding the maturity of account management controls and will assist in prioritizing improvements. The Province accepts the valuable recommendations of the Office of the Auditor General as they are well-aligned with the direction of the government identity program.

ABOUT THE AUDIT

BACKGROUND

Effective identity and access management helps keep personal and sensitive information safe

The B.C. government needs to collect information so it can provide and improve services, such as healthcare and education. The information collected is often sensitive—it can include personal health records, social insurance numbers, birth records, and personal and government financial information—so it is important to limit access to only those authorized to work with the information.

Today, almost all sensitive information is collected and stored electronically. Keeping electronic data safe requires a robust method for identifying users, determining what they can access and then controlling access appropriately. Effective identity and access management tools can help do these things, reducing the risk of sensitive information being accessed by unauthorized individuals for fraudulent purposes.

The B.C. government established a service to control access to personal and sensitive information

In the B.C. government, the Office of the Chief Information Officer (OCIO) operates within the Ministry of Citizens' Services and it leads the strategy, policy and standards for telecommunications, information technology (IT), IT security and a variety of other IT initiatives.

The OCIO's senior executive, the Government Chief Information Officer (GCIO), is responsible for ensuring that the security of government's information is maintained and protected. Therefore, the GCIO creates IT strategies and policies including the Information Security Policy (ISP).

The "Access Control" chapter of the ISP (the chapter was subsequently moved to the Information Security Standard, or ISS), provides the framework for government organizations to meet their goals to protect government information and technology assets. The "Access Control" chapter of the ISS identifies methods of controlling access to government information and information assets, and provides the blueprint for management of employee and contractor access, their authorizations and the control requirements for computer networks, operating systems, applications and information.

The GCIO established the Internal Directory and Authentication Service (commonly known as IDIR). B.C. Government ministries use the IDIR service to provide their employees and contractors with user accounts to log on to workstations and access online services. When employees and contractors log on to their computers, they are required to input their username (a unique identifier), along with their password. With this process, the IDIR service authenticates users' identities before they are granted access to government networks and applications.

ABOUT THE AUDIT

The OCIO, as the *information custodian*, is responsible for managing the IDIR service. The ministries, as *information owners*, are responsible for establishing processes to manage the many access control policies and standards, including:

- documenting processes for adding, changing and monitoring user access, and properly segregating roles and functions (i.e., access requests, access authorization and access administration)
- defining rules for controlling access to privileged system functions (i.e., access requests, access authorization and access administration)

IDIR service—the first defence against unauthorized access

The IDIR service authenticates government employees' and contractors' identities before access is granted to internal government computer resources. It is the first defence against unauthorized access to government information and information assets.

But to be effective, access to resources needs to be kept current according to users' employment or contractual status, as well as their roles and responsibilities, so as to prevent inappropriate access to government information—possibly for fraudulently use.

In the past several years, as part of our audit of government's financial statements, we reviewed government's general IT controls for network access, and noted control deficiencies in user account management at some government ministries. Control deficiencies included the following:

- User accounts were not always disabled in a timely manner after employees left and their access was no longer required.
- Some privileged users continued to have access after their job roles changed. Privileged accounts represent the highest risk because they have the highest level of access.

We reported these deficiencies to management at the Ministry of Citizens' Services in 2016 and 2017.

We found that the number of active user accounts did not match the number of government employees, and the discrepancies grew over years. There may be reasons for the discrepancies. The OCIO recognized this, and in early 2018, initiated a clean-up project to determine the validity of IDIR accounts. As part of our audit, as summarized in the last section of this report, we conducted a further analysis of IDIR user accounts to see how well the clean-up project was performed.

As government increases the sharing of information from multiple sources through its various systems, the need for proper administration of IDIR user accounts and application access management becomes even more critical.

ABOUT THE AUDIT

AUDIT SCOPE

We conducted our field work from June to August in 2018. We focused on the IDIR service managed by the Access & Directory Management Services within the Office of the Chief Information Officer of the Ministry of Citizens' Services, and related control processes of the following five ministries and their related branches and agencies (nine entities in total):

- Citizens' Services
- Finance, including the following entities:
  - Corporate Accounting Services Branch
  - Information Management Branch
  - Financial Institutions Commission
  - Provincial Treasury Branch
  - BC Public Service Agency
- Health
- Attorney General
- Forests, Lands, Natural Resource Operations and Rural Development

We selected these five ministries because they manage significant systems and have collected confidential and sensitive information.

AUDIT METHOD

The report is dated August 1, 2019. This is the date the audit team completed obtaining the evidence used to determine the findings and conclusions of the report.

We developed a set of questionnaires based on the "Access Control" chapter of the B.C. government's Information Security Standard. We sent the questionnaires to each of the five selected ministries and their related branches and agencies to self-assess their compliance to the access control chapter.

We validated their self-assessed results through the following:

- examining supporting documents provided, such as policies and procedures
- confirming the design and implementation of procedures through inquiry
- selecting a sample of transactions and following along with the auditees through the described processes

Our work was limited to confirming whether the selected ministries and their related branches and agencies' practices reflected that of Government's *Information Security Standards*. We did not test to confirm that these key controls are operating effectively.

We analyzed the IDIR accounts by comparing the IDIR accounts database with the government employees payroll database that is maintained by the BC Public Service Agency to confirm that the IDIR accounts are current.

AUDIT OBJECTIVE AND CONCLUSION

AUDIT OBJECTIVE

Our audit objective was to determine if the five selected ministries and their related branches and agencies have designed and implemented key controls as identified in the "Access Control" chapter of the B.C. government's Information Security Standard for protecting government information and information assets from unauthorized access.

AUDIT CRITERIA SUMMARY

To determine this, we asked the five selected ministries and their related branches and agencies the following five questions:

1. Is there a formal provisioning process to assign IDIR user accounts for all employees and contractors?
2. Is there a formal process to link IDIR user accounts to access ministry applications and related services?
3. Is there a formal de-provisioning process to remove IDIR user access for all employees and contractors and related services?
4. Is the use of IDIR privileged accounts restricted and controlled?
5. Are ministries formally reviewing employees' and contractors' IDIR access rights at regular intervals to ensure their access rights are current and valid?

AUDIT CONCLUSION

We concluded that the Office of the Chief Information Officer has designed key controls for protecting government information and information assets from unauthorized access as identified in government's security standards. Although the selected entities have implemented some of the controls identified by government's security standard, there are instances where key controls have not been implemented. These deficiencies increase the risk of unauthorized access to government's information systems.

Deficiencies found include an absence of:

- formal documentation of procedures for creating and removing users
- monitoring of privileged account users
- regular review of users' access rights to confirm validity

KEY FINDINGS AND RECOMMENDATIONS

Exhibit 1 is a summary of overall audit results for each ministry and its related branches and agencies by audit criteria. The results of each criterion are further explained below.

Exhibit 1: Summary of audit results for each entity by audit criteria

Ministry name	Citizens' Services	Finance					Health	Attorney General	Forests, Lands, Natural Resource Operations and Rural Development
Branch / Agency / Audit criteria		Corporate Accounting Services	Information Management Branch	Provincial Treasury	Public Service Agency	Financial Institutions Commission			
Is there a formal provisioning process to assign IDIR user accounts for all employees and contractors?	Partial	No	No	No	Partial	Partial	Yes	Yes	Yes
Is there a formal process to link IDIR user accounts to access ministry applications and related services?	Yes	Yes	No	Yes	Partial	Yes	Yes	Yes	Yes
Is there a formal de-provisioning process to remove IDIR user access for all employees and contractors and related services?	Yes	Yes	Partial	Partial	Partial	Yes	Yes	Yes	Partial
Is the use of IDIR privileged accounts restricted and controlled?	No	Yes	No	No	Partial	Yes	Yes	No	Partial
Are ministries formally reviewing employees' and contractors' IDIR access rights at regular intervals to ensure their access rights are current and valid?	No	Partial	No	No	No	No	No	No	No

Source: Office of the Auditor General of British Columbia

SETTING UP IDIR USER ACCOUNTS

Processes to assign IDIR user accounts could be enhanced

We looked at the five selected ministries and their related branches and agencies to see if the following controls were in place for IDIR user account setup (see Exhibit 2 for our results):

- formal documented procedures for creating new users
- a designated employee to administer the IDIR services
- an established segregation of duties between approval and setup of new users' IDIR accounts

KEY FINDINGS AND RECOMMENDATIONS

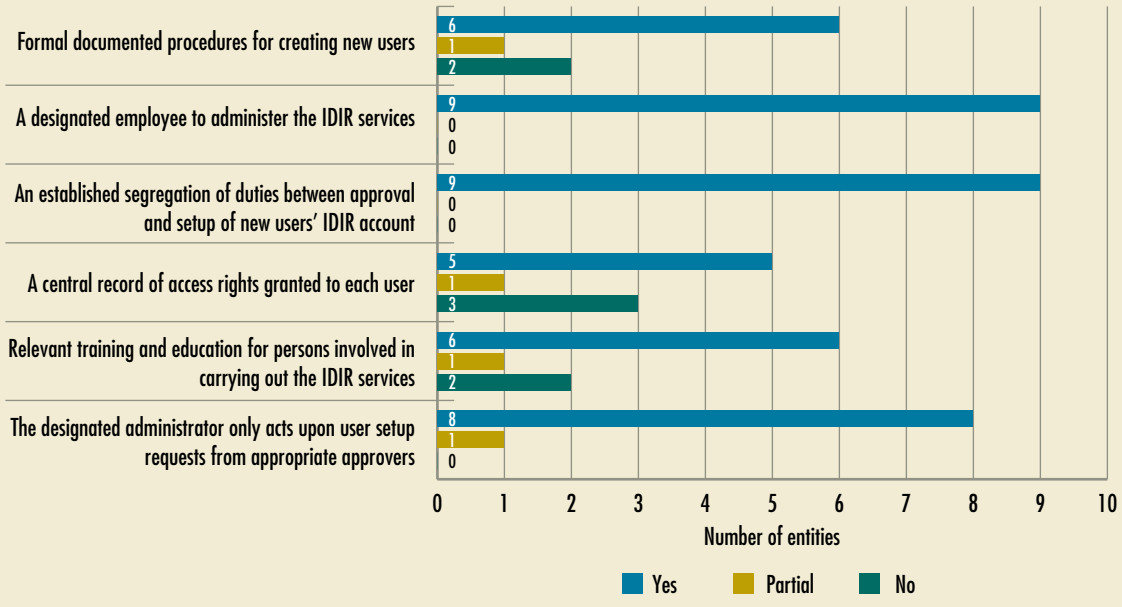
- a central record of access rights granted to each user
- relevant training and education for persons involved in carrying out the IDIR services
- the designated administrator only acts upon user setup requests from appropriate approvers

Overall, we found that most ministries and related branches and agencies had documented procedures for user creation. However, some branches within one ministry did not have their procedures documented. Since each ministry is unique in its business environment (some have decentralized branches and independent agencies operating under their responsibilities), formal, documented procedures, tailored to its business environment, will help ensure that staff clearly understand their roles and responsibilities in IDIR account creation.

All ministries and related branches and agencies had a designated employee to administer the IDIR services. The designated employees were mainly service desk staff members in the Information Management and Information Technology (IMIT) group, rather than from the business area. This establishes segregation of duties, ensuring that the requestor of an IDIR account (usually human resources within the business unit) is not also the creator of the account.

We found that ministries and their related branches and agencies were not consistent in maintaining their

Exhibit 2: Setting up IDIR user accounts



Source: Office of the Auditor General of British Columbia

own records of IDIR account users with details about access rights (i.e., *who* can access *what* applications). One branch and an agency of a ministry indicated that the OCIO should be responsible in ensuring that access rights were granted appropriately. Overall, it appears that the roles and responsibilities of maintaining a central record of access rights for IDIR user accounts are unclear between the ministries and the OCIO.

Although we noted that all designated IDIR service administrators were knowledgeable in their roles and responsibilities, not all of them received formal training and education in the process of setting up and removing IDIR user accounts.

We noted that all five ministries have a process in place to ensure that IDIR access requests were from authorized individuals. However, our inquiry and testing found one branch did not consistently follow the process. It is important that only authorized user access requests are acted upon before granting the requested access.

RECOMMENDATION 1: *We recommend that the Office of the Chief Information Officer work with ministries to:*

a) apply clear roles and responsibilities as defined for the IDIR user accounts provisioning processes

b) reconcile the Information Security Policy and Standards as they relate to the maintenance of a central record of access rights for IDIR users

RECOMMENDATION 2: *We recommend that the Office of the Chief Information Officer work with non-compliant ministries to ensure they:*

a) develop and document ministry specific procedures for setting up IDIR user accounts for new employees and contractors

b) establish a formal training and education program for those who are involved in the IDIR service

c) implement a process ensuring only properly authorized IDIR user accounts requests are acted upon

Processes for linking IDIR accounts to ministry resources could be improved

We looked to see if the five selected ministries and their related branches and agencies had the following controls in place (see Exhibit 3 for our results):

- formal and documented procedures for permitting employees' and contractors' IDIR user accounts to access ministry applications resources (e.g., Corporate Accounting Services) and other related services
- a designated employee(s) responsible for administering the linking of ministry and other government applications to IDIR user accounts
- an established segregation of duties between the authorization and setting up of IDIR user accounts in accessing ministry and other government applications

KEY FINDINGS AND RECOMMENDATIONS

- ministry IDIR account administrators only act on access requests from the appropriate ministry application(s) owner

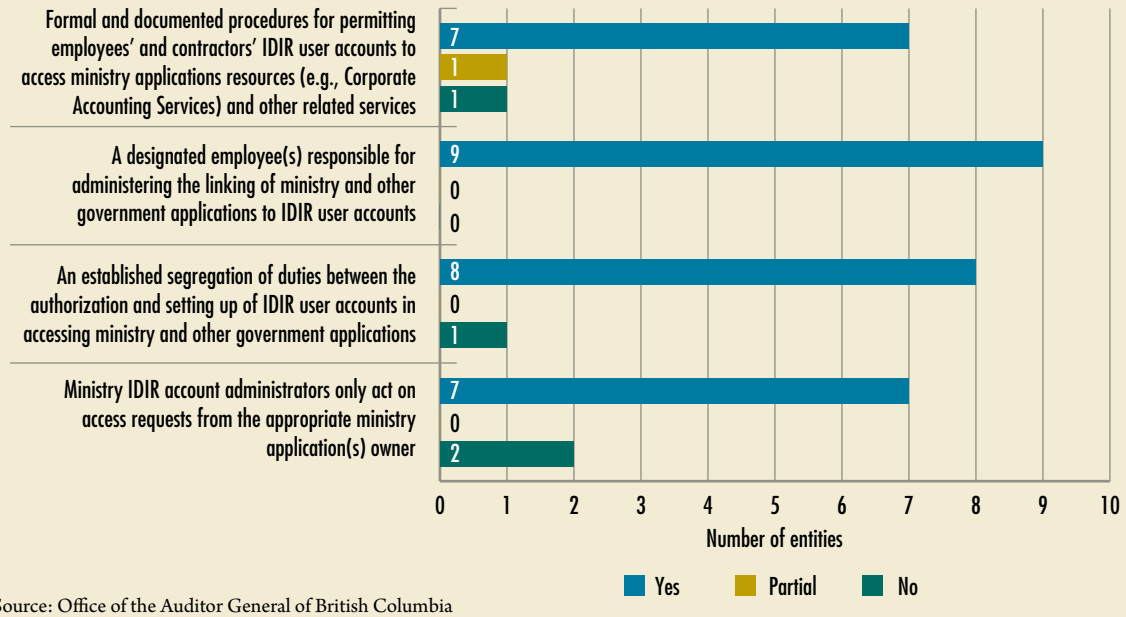
Overall, we found that four ministries had formally documented processes for setting up employees' and contractors' IDIR user accounts to access ministry applications' resources, such as government corporate accounting systems and BC Online. However, one of the branches and one of the agencies had processes that were not formally documented.

As indicated earlier, because each ministry has its own unique business requirements for access to applications and online services, it is important to have the processes clearly documented to ensure each IDIR account user is granted appropriate access.

Also important, is the segregation of duties—this is the foundation for effectively reducing opportunities to conceal errors or fraudulent activities. All ministries and related branches and agencies had designated employees to link the ministries' applications to IDIR user accounts. This ensures that the authorization of users and the setting up of IDIR user accounts are completed by independent individuals.

We found that all five ministries had processes to ensure that the IDIR administrator only acts upon authorized access requests from business owners. Through our inquiry and testing, we found that one branch's request for application access was made directly to the ministry's designated IDIR administrator, without receiving the appropriate approval by the application's business owner. Also, we found that one agency didn't have a process in place

Exhibit 3: Linking IDIR user accounts to access ministry resources



Source: Office of the Auditor General of British Columbia

for granting approval by the business owners of each application (see recommendation 2(c)).

RECOMMENDATION 3: *We recommend that the Office of the Chief Information Officer work with non-compliant ministries to ensure they develop and document ministry-specific procedures for establishing access permissions for authorized IDIR user accounts to access applications.*

Process to remove IDIR user accounts could be improved

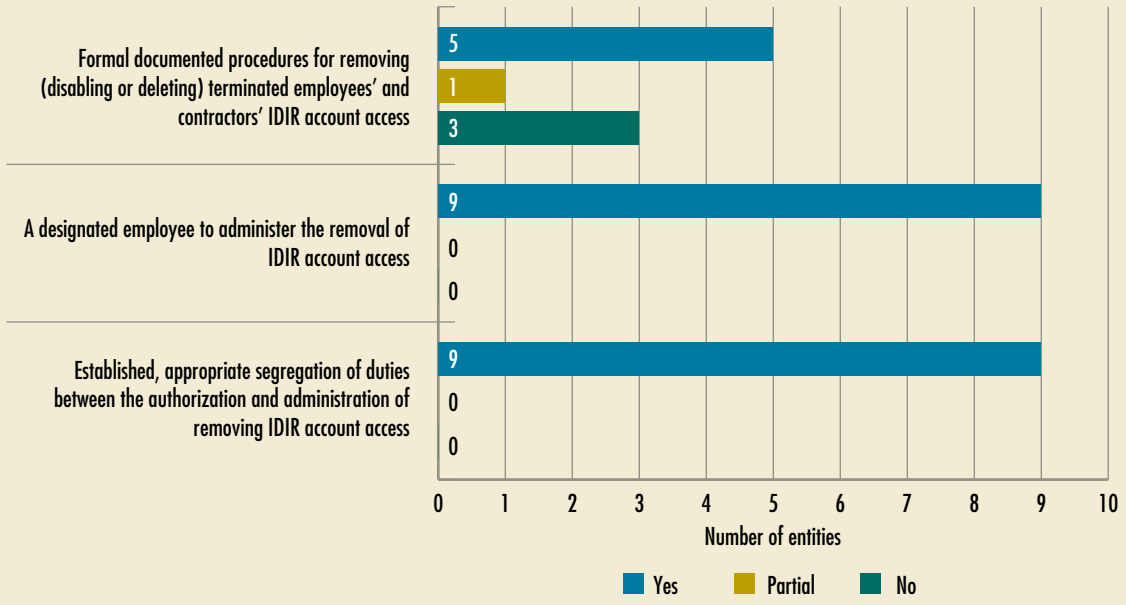
We looked to see if the five selected ministries and their related branches and agencies would have the following controls in place (see Exhibit 4 for our results):

- formal, documented procedures for removing (disabling or deleting) terminated employees' and contractors' IDIR account access
- a designated employee to administer the removal of IDIR account access
- established, appropriate segregation of duties between the authorization and administration of removing IDIR account access

Overall, we found that not every ministry had documented the procedures for removing IDIR accounts that were specific for its own business environment.

We found that all ministries, branches and agencies had designated employees to administer the removal of IDIR users' account access, and established

Exhibit 4: Process to remove IDIR user access



Source: Office of the Auditor General of British Columbia

segregation of duties between authorization and removal of terminated employees' or contractors' IDIR accounts.

RECOMMENDATION 4: *We recommend that the Office of the Chief Information Officer work with non-compliant ministries to ensure they develop and document ministry-specific procedures for the removal of IDIR user accounts of terminated employees and contractors.*

Privileged IDIR accounts were restricted and controlled, but not managed according to the access policy

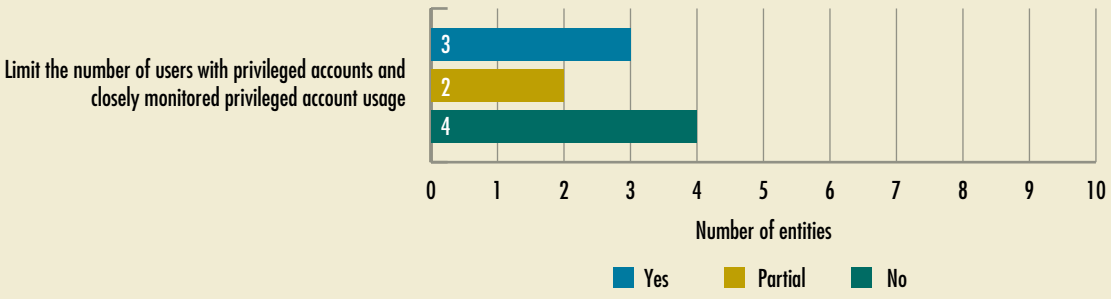
We looked to see if the five selected ministries and their related branches and agencies limited the number of users with privileged accounts and closely monitored privileged account usage (see Exhibit 5 for our results).

Privileged IDIR accounts are for employees who have been granted special privileges, such as the ability to make changes to other IDIR accounts (e.g., reset a password or alter what the account has access to). Privileged accounts are mainly assigned to (but are not limited to) people working as system administrators, network administrators, database administrators, security administrators, system operators and network operators. Because privileged accounts are powerful, their assignment and use must be restricted and controlled.

Overall, we found that the ministries and their related branches and agencies had processes in place to assign and restrict the number of privileged user accounts. However, we found that only one ministry and two entities from another ministry monitored to ensure privileged IDIR account activities were appropriate and authorized.

RECOMMENDATION 5: *We recommend that the Office of the Chief Information Officer work with non-compliant ministries to ensure they establish processes for reviewing privileged IDIR account users' access rights and monitoring their activities to ensure they are appropriate and authorized.*

Exhibit 5: Restriction and control of privileged IDIR accounts



Source: Office of the Auditor General of British Columbia

KEY FINDINGS AND RECOMMENDATIONS

IDIR accounts' access rights weren't reviewed at regular intervals

We looked to see if the five selected ministries and their related branches and agencies had the following controls in place (see Exhibit 6 for our results):

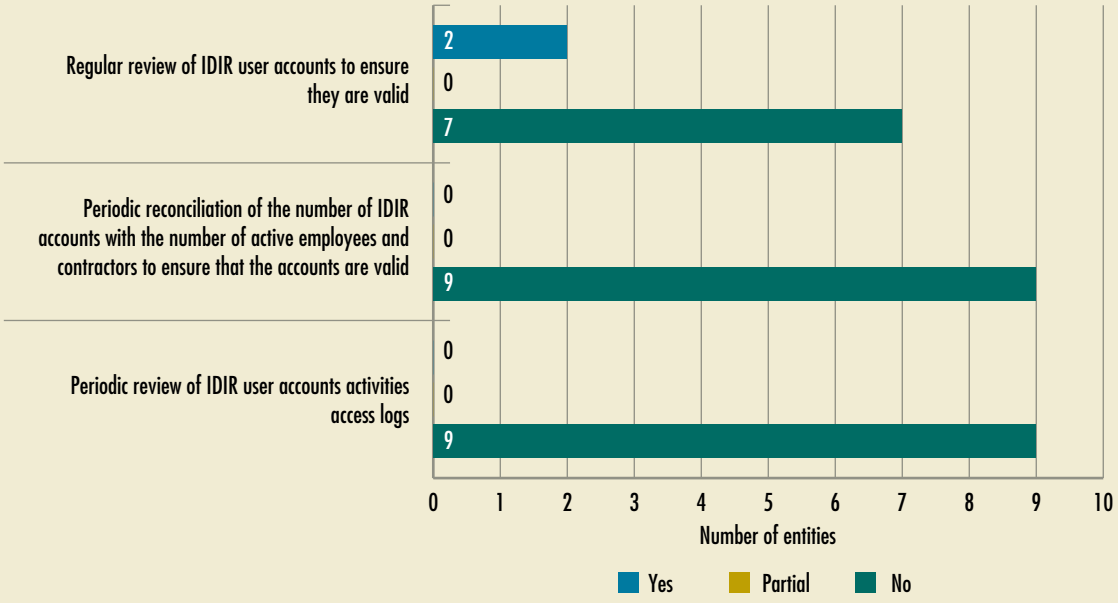
- regular review of IDIR user accounts to ensure they are valid
- periodic reconciliation of the number of IDIR accounts with the number of active employees and contractors to ensure that the accounts are valid
- periodic review of IDIR account activities access logs

Employment status and contractor terms change often. Some examples of what could affect the access privilege status of IDIR accounts include:

- employees getting promoted or moving to different ministries or departments
- employees retiring
- employees being terminated
- contractors' terms expiring
- contractors' work purpose changing

We found that only one branch and one agency regularly reviewed their IDIR user accounts for validity. The rest did not perform periodic reconciliations of the number of IDIR accounts with the number of active employees and contractors to ensure that the accounts were valid.

Exhibit 6: Review of IDIR account access rights



Source: Office of the Auditor General of British Columbia

KEY FINDINGS AND RECOMMENDATIONS

The OCIO's security investigations group reviews the IDIR activities' logs in response to security incidents. This monitoring activity mitigates the risk of current employees and contractors being given an inappropriate level of access. However, it is not effective enough, as it is only acted upon when security incidents occur.

We found that the number of IDIR accounts did not reasonably match the number of government employees in the employee payroll database (commonly known as CHIPS). On January 4, 2018, the OCIO had initiated a clean-up project to determine the validity of IDIR accounts and asked each ministry to review and remove IDIR accounts that were considered unused (dormant) for a long period of time and accounts that had expired passwords.

On February 1, 2018, the OCIO initiated a project to delete dormant IDIR user accounts and on August 13, 2018, the OCIO announced that it will continue to run the dormant accounts clean-up process monthly, and that the ministry's IT service managers will be expected to review the OCIO's reports and take appropriate action. All five ministries have implemented this process.

We believe this is a good start; however, we found that the scope of the process did not include the review of current employees' and contractors' statuses to determine whether:

- their IDIR accounts were still valid
- their access level continued to be appropriate
- the password expiry term of each account is adhering to government password configuration policy

In order to see how well the clean-up was performed, we analyzed the IDIR accounts by comparing the IDIR accounts database with the government employee payroll database that is maintained by the BC Public Service Agency. We based our comparison on data obtained as of June 20, 2018 (after the clean-up project). We found discrepancies and have summarized them, along with the associated risks, in Exhibit 7.

Although the number of discrepancies we found was small relative to the total number of IDIR accounts, even a single poorly managed IDIR account could lead to fraud or to compromised government information and systems.

RECOMMENDATION 6: *We recommend that the Office of the Chief Information Officer work together with the BC Public Service Agency to compare the IDIR user employee profiles with the government employee payroll database and where discrepancies are identified make the appropriate corrections.*

RECOMMENDATION 7: *We recommend that the Office of the Chief Information Officer work with ministries to expand the scope of the monthly review of IDIR user accounts to include checking for non-expiring password settings and IDIR accounts that have remained active, even after employees and contractors no longer work for government.*

KEY FINDINGS AND RECOMMENDATIONS

Exhibit 7: Results of OAG analysis of IDIR user accounts

Findings from IDIR account analysis	Risks associated
Comparison with government payroll database (CHIPS)	
We found 237 IDIR user accounts where the employees' ministry that was recorded in the IDIR user account was not the same as the employees' ministry name in CHIPS. The breakdown of the 237 users is: 160 – Active employees, 12 – On leave, 6 – Retired, 59 – Terminated	The risk of IDIR users having access to the wrong ministry services is low since access to authorized ministry services is based on other configurations within the program that manages permissions and access to networked resources. However, the discrepancies noted indicate that there is a lack of reconciliation between IDIR accounts and payroll databases with regard to the current employee profile.
We found 114 IDIR accounts where the associated employee name differed from the corresponding name in the CHIPS database, even though the employee IDs matched. It is unclear whether the employee names were incorrect, or the employee IDs were incorrect.	Having multiple or inconsistent employee and contractor names associated with a single employee ID may create these risks: ◆ the right person may be given too much access (though a combination of permissions meant for two people) ◆ the wrong person may be given access (through permissions meant for someone else)
We found there were 538 IDIR accounts used after user employment status was non-active.	Users that should no longer have access may still have access to government computer resources and information. This could result in unauthorized access and sensitive information being used for fraudulent activities.
We found 712 IDIR account users on leave who still had enabled IDIR accounts. The following is a breakdown by year: 2015 = 1, 2016 = 8, 2017 = 69, 2018 = 634	Enabled accounts for users on leave presents a variety of threat scenarios. Confidentiality risk aside (users may be able to view data not meant for them during their leave), even the availability of the account means someone who discovers the password while the user is on leave can use the account for a variety of risky purposes (e.g., email impersonation or snooping) with little chance of being stopped.
Other findings	
We found that 133 IDIR accounts had a non-expiring password setting.	Passwords should not remain the same forever. This is because passwords can become known to malicious individuals without the IDIR user having any knowledge of the compromise. Examples include: ◆ where an IDIR account holder has reused the password on another system, such as an eCommerce or gaming site, and the passwords are breached at *that* site ◆ malware gets onto to an IDIR user's computer and steals the password directly Regardless, when a password has become known, it creates confidentiality and data integrity risks for any data the IDIR user has access to (e.g., social insurance numbers).
We found 738 IDIR accounts that had not been used since 2017 and some were from 2009.	Obsolete accounts that are still enabled will increase the risk of information and systems being compromised and misused.

Source: Office of the Auditor General of British Columbia

AUDIT QUALITY ASSURANCE

We conducted this audit under the authority of section 11 (8) of the *Auditor General Act* and in accordance with the standards for assurance engagements set out by the Chartered Professional Accountants of Canada (CPA) in the *CPA Canada Handbook*—Canadian Standard on Assurance Engagements (CSAE) 3001 and Value-for-money Auditing in the Public Sector PS 5400. These standards require that we comply with ethical requirements, and conduct the audit to independently express a conclusion on whether or not the subject matter complies in all significant respects to the applicable criteria.

We apply the CPA Canadian Standard on Quality Control 1 (CSQC), and accordingly, maintain a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements. In this respect, we have complied with the independence and other requirements of the code of ethics applicable to the practice of public accounting issued by the Chartered Professional Accountants of British Columbia, which are founded on the principles of integrity, objectivity and professional competence, as well as due care, confidentiality and professional behaviour.

APPENDIX A: COMPLETE AUDIT CRITERIA

1. Is there a formal provisioning process to assign IDIR user accounts for all employees and contractors?
    - formal documented procedures for creating new users
    - a designated employee to administer the IDIR services
    - an established segregation of duties between approval and setup new users' IDIR accounts
    - a central record of access rights granted to each user
    - relevant training and education for persons involved in carrying out the IDIR services
    - the designated administrator only acts upon user setup requests from appropriate approvers
2. Is there a formal process to link IDIR user accounts to access ministry applications and related services?
    - formal and documented procedures for permitting employees' and contractors' IDIR user accounts to access ministry applications resources (e.g. Corporate Accounting Services) and other related services
    - a designated employee(s) responsible for administering the linking of ministry and other government applications to IDIR user accounts
    - an established segregation of duties between the authorization and setting up of IDIR user accounts in accessing ministry and other government applications
    - ministry IDIR service administrators only act on access requests from the appropriate ministry application(s) owner
3. Is there a formal de-provisioning process to remove IDIR user access for all employees and contractors and related services?
    - formal documented procedures for removing (disabling or deleting) terminated employees' and contractors' IDIR account access
    - a designated employee to administer the removal of IDIR account access
    - established appropriate segregation of duties between the authorization and administration of removing IDIR account access
4. Is the use of IDIR privileged accounts restricted and controlled?
    - limit the number of users with privileged accounts and closely monitor privileged account usage
5. Are ministries formally reviewing employees' and contractors' IDIR access rights at regular intervals to ensure their access rights are current and valid?
    - regular review of IDIR user accounts to ensure they are valid
    - periodic reconciliation of the number of IDIR accounts with the number of active employees and contractors to ensure that the accounts are valid
    - periodic review of IDIR user accounts activities access logs

AUDIT TEAM

Cornell Dover,
Deputy Auditor General

David Lau,
Director, IT Audit

Pam Hamilton,
Director, IT Audit

Alan Swiatlowski,
IT Auditor

Ravi Madappattu,
IT Auditor

Jenny Wang,
IT Auditor

OFFICE OF THE
Auditor General
of British Columbia

Location

623 Fort Street
Victoria, British Columbia
Canada V8W 1G1

Office Hours

Monday to Friday
8:30 am – 4:30 pm

Telephone: 250-419-6100
Toll free through Enquiry BC at: 1-800-663-7867
In Vancouver dial: 604-660-2421

Fax: 250-387-1230

Email: bcauditor@bcauditor.com

Website: www.bcauditor.com

This report and others are available at our website, which also contains further information about the office.

Reproducing

OFFICE OF THE
Auditor General
of British Columbia