REPORT ON:

User Access Management

IAAS | INTERNAL AUDIT & ADVISORY SERVICES

BRITISH COLUMBIA | Ministry of Finance

Introduction

The Government of British Columbia (Province or Government) collects and manages a large amount of personal and sensitive electronic information. This information is an asset that is collected for, and owned corporately by, the Province. The Government has a responsibility to protect the confidentiality, integrity and availability of the information assets it holds. Therefore, the Government must ensure that only authorized users can access this information.

Access control processes should be in place, and effective practices should be followed to adequately protect the Government from security threats. Access controls manage user identities and related access permissions to an organization's information and systems.

For most users in Government, access to government shared drives, networks and applications are administered through the Government's internal directory account service (IDIR). IDIR authenticates the identity of employees and contractors with user accounts, allowing them to log onto computer workstations and to access some government information systems. IDIR user authentication is the overall responsibility of the Office of the Chief Information Officer (OCIO), Ministry of Citizens' Services. Ministries are responsible for managing employee and contractor user access once granted.

Some information system authentication processes are not integrated with IDIR ('non-IDIR' systems) due to system capabilities, or because they are intended to provide access to a broader variety of users (e.g. members of the public). User authentication for these systems is often managed by ministry business units leading to a decentralized process. This can increase the risk of providing unauthorized access, which may impact the confidentiality and integrity of data in these systems.

The OCIO provides guidance to ministries on the management of user access through the Access Control Security Standard (ACSS). The ACSS outlines controls and practices to protect government information and technology assets. Ministries are responsible for managing access to their systems by ensuring that appropriate controls are in place. Access controls can reduce the risk of a disruption to information systems, for instance, unauthorized or unintentional modification or misuse.

Review Summary

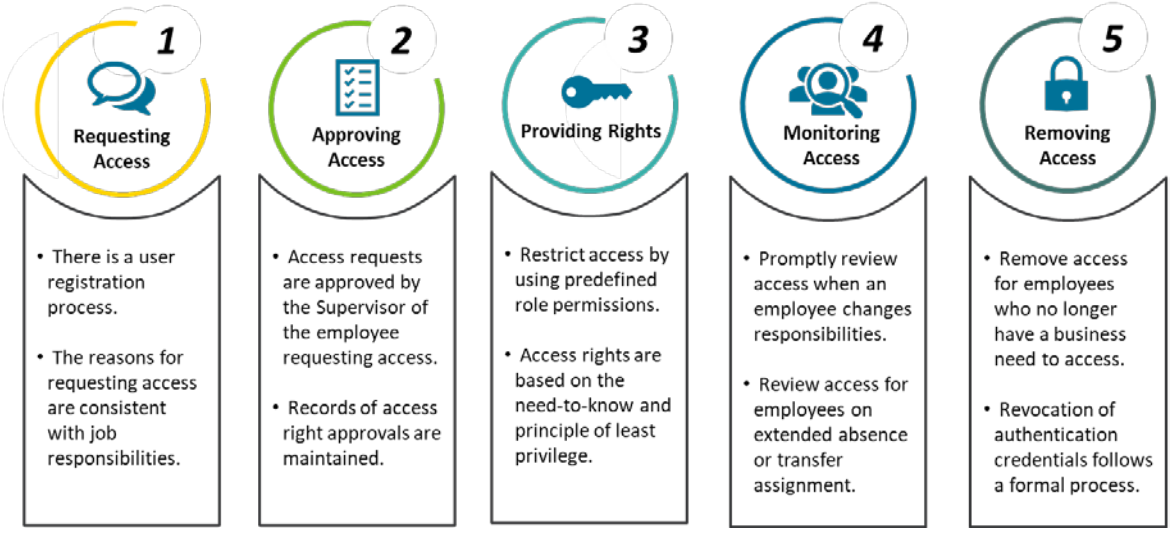
Internal Audit & Advisory Services reviewed whether appropriate user access processes are in place and are followed for seven non-IDIR information systems from the Ministry of Finance and the Ministry of Education. The review selected a sample of critical business systems that do not integrate with IDIR for authentication.

The review evaluated and made recommendations, where appropriate, on the ministries' user access management processes, with a focus on the following areas:

- **Alignment with the Access Control Security Standard:** user access processes within ministry business areas, including alignment with the OCIO standard and communication to ministry staff.
- **Operations:** user access practices, including granting, removing and monitoring are operating as intended.

Internal management reports, with detailed recommendations, were issued to the ministries reviewed. Due to the sensitivity of the review's scope, the details of these reports will not be publicly released.

The ACSS provides guidance for the implementation of key access controls based on the risk associated with the system. The following summarizes the key controls introduced in the ACSS.



Source: IAAS developed based on the Access Control Security Standard

The majority of the systems reviewed had specific procedures outlining good practices for user access management. Such practices included:

- defining roles and responsibilities;
- a process for granting, modifying and removing access;
- timelines for access removals, for instance after a system user changed position or left Government; and
- a schedule for monitoring user access.

Conclusion

The OCIO has established a common framework to ensure adequate procedures and controls are in place to protect government information and technology assets. The Ministry of Finance and the Ministry of Education generally have controls in place to manage their access; however, there are opportunities for the ministries reviewed to improve on the application of these controls in specific areas.

We identified five recommendations relevant to each ministry and two ministry-specific recommendations relating to the following:

- Two recommendations relating to developing or enhancing policy and/or procedural guidance and communicating access management practices to key stakeholders.
- Two recommendations relating to enhancing the processes supporting timely removal or modification of system user access.
- One recommendation relating to strengthening user access monitoring processes.
- Two recommendations relating to strengthening controls for privileged user accounts.

The ministries reviewed have developed actions plans to address these recommendations.

While this review focused on two ministries, our review has relevance across all of Government, and we encourage other ministries to review their user access management with good practices as outlined in the ACSS.

* * *

We would like to thank the ministry staff, who participated in and contributed to, this review for their cooperation and assistance.

Stephen Ward, CPA, CA, CIA
Executive Director
Internal Audit & Advisory Services
Ministry of Finance