



City of Edmonton Office of the City Auditor

Access to Digital Assets

December 16, 2019

Username

Password

Remember Me



Login

Register



1200, Scotia Place, Tower 1
10060 Jasper Avenue
Edmonton, AB T5J 3R8
Phone: 780-496-8300
edmonton.ca/auditor



About Access to Digital Assets

What is a digital asset?

A digital asset is an information technology resource that the City uses to achieve its business objectives.

Digital information, and supporting technology, as well as operational technology (such as health and safety systems) are examples of digital assets.

What is Access Control?

Access Controls can be physical or logical.

Physical access controls are activities that prevent someone from entering a facility or space. The best example is a locked door which can only be opened with a key or scan card.

Logical access controls are activities that prevent someone from accessing all or some of the internal information / capabilities of a digital asset.

Why do logical access controls matter?

Logical access controls¹ ensure that people have enough information and enabling capabilities from a digital asset to do their work – no more and no less.

Too much access means that people may see information or use capabilities they are not supposed to see or use. This puts the City at higher risk for system failure of digital assets, information theft, and other issues that can negatively affect the corporation and citizens.

Too little access means that people may not be able to do their work efficiently or effectively. This also affects the City negatively, through lower productivity and inadequate provision of services to citizens.

Why was this audit performed?

Access control activities should be well-designed and properly implemented. Doing so ensures that the right people have the right access to carry out the City's business.

¹ Hereafter, logical access controls will be referred to as access controls in the report.

Audit Objectives

Governance

To determine if the governance and oversight for access to digital assets is adequate and effective.

Access Control Processes

To determine if access control processes (and procedures) are designed and applied consistently to safeguards access to digital assets.

Risk Management

To determine if risks to access control are identified, assessed, and addressed on an ongoing basis.

Scope

The period under review was January 1, 2014 to December 31, 2018. Our assessment of access control was limited to logical access control. Physical Access Control (e.g., entry to facilities) was not in scope for this audit.

The City's governing framework for access control during the period was reviewed. From a detailed risk assessment, the following five digital assets were also selected to perform tests of compliance with the governing framework.

Digital Assets Reviewed
Emergency Services Dispatch System
Traffic Control System
ETS Control System
Human Resources Analytics Reporting System
File Management System

Statement of Professional Practice

This project was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.



Governance Review

Governing framework for access control

From January 1, 2014 to December 31, 2018, guidance on providing adequate access control to digital assets was provided in the City of Edmonton's Cyber Security Technical Standard #5: *Access Control* (Access Control Standard).

This standard was a component of the City's larger effort to manage the City's information via the Information Management Administrative Directive (A1461).

City of Edmonton Information Management Administrative Directive and Procedure (A1461)
City of Edmonton Cybersecurity Technical Standards
1. Organization of Cyber Security
2. Asset Management
3. Physical and Environmental
4. Communications and Operations Management
5. Access Control
6. Acquisition, Development, and Maintenance
7. Cyber Security Incident Management
8. Business Continuity Management

Alignment with ISO

The City of Edmonton's Access Control Standard was designed by the Open City & Technology Branch to align with ISO², an established source for best practices in a variety of business processes, including information technology.

ISO suggests 13 access control activities that should be reflected in a guiding document for access controls³. The City's Access Control Standard was reviewed for alignment with ISO's suggested guidance.

² ISO stands for the International Organization for Standardization.

³ ISO Standard 27002-2013, Chapter 9: Access Control

Summary of findings

The City's 2014 Access Control Standard generally aligns with ISO suggested guidance. It addresses several critical access control activities including:

1. The requirement that Asset Owners develop and document an access control process for their digital assets. Doing so ensures that access to a digital asset is consistently administered.
2. The requirement that access to a digital asset is limited to a user's job requirements. This ensures that inappropriate access to a digital asset is not granted.
3. The requirement that password management processes result in quality passwords. This ensures that passwords, being the first point of entry into a digital asset, are not easily guessable, frequently changed, and are appropriately secured.

Two gaps between the City's 2014 Access Control Standard and ISO suggested guidance were identified. Appendix 1 contains the comparison of the 2014 Access Control Standard to ISO.

Exceptions to alignment with ISO

Unaddressed Provisions

Two important access control activities suggested by ISO were missing in the 2014 City's Access Control Standard:

1. Restricting access to program source code – which controls how a digital asset should work; and
2. Restricting access to utility programs – these are background programs within a digital asset, which maintain and can often override key functions of that digital asset.

Both provisions are important to minimizing inappropriate access to digital assets and should therefore be reflected in the City's guidance for access control.

2019 Access Control Standard

In January 2019, the Open City & Technology Branch updated the 2014 Access Control Technical Standard as part of a new governing framework for Cyber Security Management. The updated version aligns completely with ISO's guidance.

As a governing document, the new 2019 Access Control Standard is appropriately broad. It focuses on the 13 access control activities without specifically prescribing how they should be implemented by Asset Owners. This is important as each digital asset is built differently and operates with a different purpose.

The digital assets reviewed as part of this audit identified pervasive weaknesses with the access control activities put in place by Asset Owners (see "Access Control Processes" section). A root cause of these weaknesses was limited understanding of access control and the risks it is meant to address.

For each of the 13 access control activities, ISO provides additional guidance that discusses the control activity and provides suggestions on how it can be implemented. Through this information, the purpose of the access control activity and the risk it is meant to deter is clear. This information is beneficial as it can enable an Asset Owner to understand, determine, and implement the most appropriate access controls for their digital asset(s).

At the conclusion of the audit, the Open City & Technology Branch updated the 2019 Access Control Standard to include a reference to ISO's implementation guidance, for the benefit of Asset Owners. However, the City's Cyber Security Administrative Directive emphasizes that access control risks, and the selection of activities to address them, are owned and are to be managed by Asset Owners.

Awareness of the governing framework for access control

Asset Owners and Access Control Managers⁴ were interviewed to determine their awareness of the Access Control Standard and their related roles and responsibilities. Both groups indicated that they were not aware of the 2014 Access Control Standard. As will be shown later, this unawareness contributed to inconsistent access control practices across the five digital assets reviewed.

According to Open City & Technology Branch management, the Access Control Standard was shared with Asset Owners when it was first released. It was also shared with business areas whenever the Open City & Technology Branch was contacted for project assistance. Aside from this, a proactive mechanism to regularly inform Asset Owners of their access control responsibilities did not exist.

Given the pace of change in the City's leadership structure since 2014, regular reminders can help Asset Owners be continuously aware of their responsibilities to protect and safeguard access to their digital assets.

See Recommendation 1

⁴ Access Control Managers are individuals that have been delegated responsibility from an Asset Owner to manage access to a digital asset.



Access Control Processes

Review of Access Control Processes

The access control processes of five important digital assets were reviewed. The goal was to assess alignment of the access control processes to the 2014 Access Control Standard. Access profiles of 100 users across the five digital assets were randomly selected and reviewed. The goal was to determine if the access each user had was approved and limited to the requirements of their job.

Table 2: Digital Assets Reviewed

Digital Assets Reviewed
Emergency Services Dispatch System
Traffic Control System
ETS Control System
Human Resources Analytics Reporting System
File Management System

Summary of findings

Provisions from the 2014 Access Control Standard are not being properly applied. This can increase the risk of inappropriate access to the digital assets. Weaknesses include inadequate password management processes, minimal review of access rights, and minimal reviews of access control processes. Asset owners should correct the identified weaknesses with the access control processes for their digital assets. Doing so would enable them to reduce and monitor risks to access control.

Table 3 aggregates and summarizes the findings across the five digital assets reviewed. Individual and detailed results were disclosed separately to each Asset Owner.

Table 3: Summary of Results – Review of Access Control Processes of Five Digital Assets

Key Access Control Activities From the City's 2014 Access Control Standard	Observation
<p>Documented Access Control Processes <i>Documented access control processes ensure that access is administered consistently and appropriately.</i></p>	<p>2/5 (40%) Of digital assets reviewed had this control in place</p>
<p>Documented Approvals <i>Access rights are approved by an appropriate individual.</i></p>	<p>40/100 (40%) Of samples reviewed had this control in place</p>
<p>Need-to-know/Least Privilege <i>Access provided is limited to fulfilling job requirements.</i></p>	<p>80/100 (80%) Of samples reviewed had this control in place</p>
<p>Regular Review of Access Rights <i>Regular review of access rights ensures ongoing appropriateness of access.</i></p>	<p>1/5 (20%) Of digital assets reviewed had this control in place</p>
<p>Password Management <i>Password processes ensure that quality passwords are developed and updated regularly.</i></p>	<p>2/5 (40%) Of digital assets reviewed had this control in place</p>
<p>Risk Management <i>Risks to access control for the digital asset are proactively identified, mitigated, and monitored on a regular basis.</i></p>	<p>0/5 (0%) Of digital assets reviewed had this control in place</p>

Common weaknesses and challenges

There are several common weaknesses and challenges across the five digital assets:

Lack of awareness of the Access Control Standard

Asset Owners and their Access Control Managers were not aware of the 2014 Access Control Standard. As a result, access control processes are inconsistent and vary across the digital assets reviewed. Further, existing processes do not always ensure that access to the digital assets remain appropriate. Asset Owners should familiarize themselves with the City's Access Control requirements. This will enable them to ensure that access controls for their digital assets are adequately designed.

Limited appreciation for Access Control risks

There is a limited appreciation for the risks that access controls are meant to protect. This was demonstrated through the existence of weak password requirements, irregular review of the access rights granted to privileged users,⁵ and poor documentation justifying a user's access. These weaknesses increase the risk of inappropriate access to digital assets.

System capabilities

The way a digital asset is designed is also a factor in how well Asset Owners can implement the City's Access Control guidance. For example, two digital assets reviewed could not generate reports on the access activities of privileged account users. User activity reports can help to identify instances of inappropriate access. Asset Owners should engage the Open City & Technology Branch if their digital assets lack such capabilities.

Nature of business

Operational requirements also make implementing aspects of the City's Access Control guidance challenging. For example, the "time-out session" provision could not be implemented for two digital assets reviewed due to the need for operators to continuously monitor critical activity. In these circumstances, Asset Owners should engage the Open City & Technology Branch to implement alternative methods of compliance.

See Recommendation 2

⁵ A privileged user is a profile account that has significant and potentially compromising system rights and powers. Privileged users, for example, may be granted the ability to change a critical system function, add/delete/modify access, etc.



Risk Management Process Review

Risk Management for Access Control

An access control risk management process helps identify, mitigate, and monitor risks to access control. The goal is to ensure that ongoing access to a digital asset remains appropriate.

Senior management from the Open City & Technology Branch, Asset Owners, and Access Control Managers, were interviewed to determine if activities were in place to support effective risk management for access control.

Summary of findings

Currently, there is no regular, systematic process for Asset Owners to communicate access control risks to the Open City & Technology Branch. This limits the ability of the corporation to collect information on key risks to access controls across the City's different digital assets. A mechanism to facilitate regular reporting could address this gap and at the same time enable Asset Owners to be regularly reminded of their access control roles and responsibilities.

Governance processes

Between 2014 and 2018, a formal program to proactively identify and address access control risks did not exist at the governance level. Rather, the Open City & Technology Branch was informed of Access Control risks on an ad-hoc basis, when contacted by business areas. Additionally, performance metrics to monitor compliance to the 2014 Access Control Standard were not developed. As a result, meaningful information did not exist to assess how well the 2014 Access Control standard was being implemented by business areas, and how well access control risks were being managed across the City's digital assets.

In January 2019 the Open City & Technology Branch developed performance metrics to monitor access control risks; however, this is only performed for a limited number of digital assets. Using performance metrics at the governance level represents a practical method of monitoring risks to access control.

Another mechanism is a regular reminder to Asset Owners, which can also be used to collect information on key risks to access control. This will provide more complete information to the Open City & Technology Branch about access control risks across the City's different digital assets.

Business area processes

Risk management processes to identify, address, and monitor risks to access control do not exist for the five digital assets reviewed. Two common and limiting factors were:

1. **Process awareness gap:** Access Control Managers are unsure about which access control risks they should be tracking and who to contact with this information.
2. **System capabilities:** Some of the digital assets reviewed cannot produce reports that summarize access control activities, or cannot do so in a meaningful or useful way. Summary reports are important as they provide useful information on legitimate and illegitimate access activity.

A regular reminder to Asset Owners can also assist with addressing these gaps. The Open City & Technology Branch can provide information to Asset Owners (and their Access Control Managers) about what risks they should be monitoring. Through this mechanism, business areas can also inform the Open City & Technology Branch of any system limitations preventing them from monitoring risks to access control.

See Recommendation 1



Recommendation 1

Regularly inform Asset Owners about their access control responsibilities.

Recommendation

Implement a mechanism to regularly inform Asset Owners of their access control responsibilities, including the responsibility to identify, address, and monitor access control risks related to their digital assets. This mechanism should facilitate the confirmation of:

1. The Asset Owner's accountability for implementing the City's requirements for access control; and,
2. The Asset Owner's responsibility to inform the Open City & Technology branch of access control risks they identify.

This mechanism should also provide guidance on the type of access control risks Asset Owners should be monitoring and reporting to the Open City & Technology branch.



Responsible party

Corporate Information Security Officer,
Open City & Technology Branch



Accepted

Management Response

The Cyber Security Administrative Directive addresses the accountabilities of Asset Owners (Branch Manager or Deputy City Managers or City Managers). During the rollout, the Administrative Directive was socialized with the Executive Leadership Team and each of the Departmental Leadership Teams. The Corporate Information Security Office will regularly remind the Asset Owners via an emailed memo of their accountabilities related to Cyber Security including access control, access control risks, as well as the availability of access control guidance from the Corporate Information Security Office.

Recommendation 2

Correct identified weaknesses with access control processes



Implementation:

February 2020

Recommendation

Address the access control weaknesses identified in accordance with the City's requirements for access control.



Responsible party

Asset Owner of each digital asset reviewed.



Accepted

Management's Responses

The Asset Owners have accepted the recommendations.
















Implementation:

October 31, 2020



Appendix One: Alignment of the City's 2014 Access Control Standard to ISO Guidance

ISO's suggested provisions for an Access Control Standard/Guideline	Is the provision discussed/referred to in the City's 2014 Access Control Standard?	Gaps or Issues?
<p>Documented access control process <i>An access control procedure should be established, documented, and reviewed based on business and information security requirements.</i></p>		None
<p>Access to networks and networks services <i>Users should only be provided with access to networks and network services they need to fulfill job requirements.</i></p>		None
<p>User registration/de-registration <i>A formal user registration and de-registration process should be implemented to enable assignment of access rights.</i></p>		None
<p>User access provisioning <i>A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services.</i></p>		None
<p>Management of privileged access rights <i>The allocation and use of privileged access rights should be restricted and controlled.</i></p>		None
<p>Management of secret authentication information of users <i>The allocation of secret authentication information should be controlled through a formal management process.</i></p>		None
<p>Review of User Access <i>Asset Owners should review users' access rights at regular intervals.</i></p>		None

ISO's suggested provisions for an Access Control Standard/Guideline	Is the provision discussed/referred to in the City's 2014 Access Control Standard?	Gaps or Issues?
<p>Use of secret authentication information <i>Users should be required to follow the organization's practices for the use of secret information.</i></p>		None
<p>Information access restriction <i>Access to information and application system functions should be restricted in accordance with the access control procedure.</i></p>		None
<p>Secure log-on procedures <i>Where required by the access control procedure, access to digital assets should be controlled by a secure log-on procedure.</i></p>		None
<p>Password management system <i>Password management systems should ensure quality passwords.</i></p>		None
<p>Use of privileged utility programs <i>Utility programs within digital assets that can override system and application controls should be restricted and tightly controlled.</i></p>		<p>Guidance is not provided. Asset Owners should consider and determine the controls required to restrict access to the utility programs in their digital assets.</p>
<p>Access control to program source code <i>Access to program source code should be restricted.</i></p>		<p>Guidance is not provided. Asset Owners should consider and determine the controls required to limit access to program source code.</p>