City of Edmonton
Office of the City Auditor

Cloud Computing Audit

January 26, 2021

Edmonton

1200, Scotia Place, Tower 1
10060 Jasper Avenue

Edmonton, AB T5J 3R8
Phone: 780-496-8300
edmonton.ca/auditor

Report Highlights

Audit Objectives

Governance
To determine if the City's cloud computing policies are in line with best practices.

Control Effectiveness
To determine if there are any control deficiencies that could negatively impact the organization.

Scope

Our review of cloud computing policies was based on documentation available as at June 30, 2020. For purposes of this audit and work performed around the Governance Objective, "policies" were considered to be any official City of Edmonton document relevant to the use of cloud services (e.g., Directives, Standards, Specifications, Requirements or other published guidance documents).

Cloud computing services can be broken down further into separate categories, depending on the nature of the arrangements. Our project focused on Software-as-a-Service (SaaS) cloud services, and specifically those that are not operated by the Open City and Technology Branch.

We did not perform testing related to the actual operations of the cloud computing vendors.

Please see **Appendix – Audit Scope** for additional scoping details, including limitations to our intended testing approach.

Statement of Professional Practice

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

About the Cloud Computing Audit

What is cloud computing

Cloud computing is a model for enabling access to a shared pool of computing resources, with those resources being managed by a different organization than the one accessing them.

Traditional Computing Model

In the past, almost all IT functions were managed using in-house resources. This means that the organizations maintained space for data centres, purchased computer servers and application software, and looked after all aspects of keeping those things up to date. City data would be stored on its own, within facilities that the City has exclusive use of.
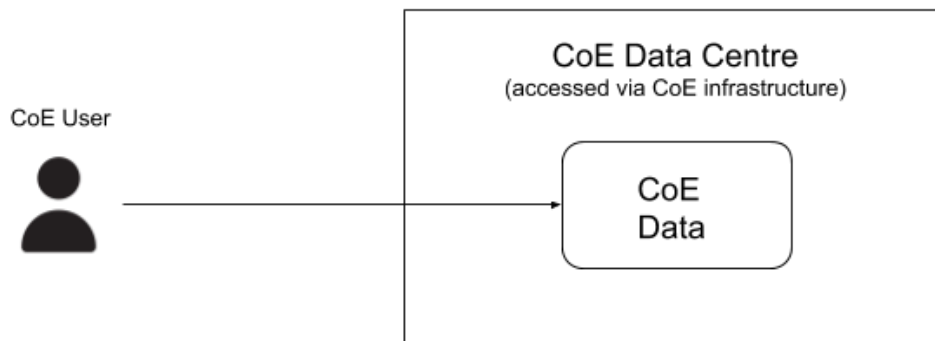
Cloud Computing Model

Today, some of the City's services and equipment related to those IT functions are managed externally through cloud computing arrangements, where the City pays a vendor to look after those pieces of the operations. Often with cloud computing, all that is required on the user's side is a computer and a connection to the Internet. City data can be stored alongside data from other companies, outside of City-run facilities.
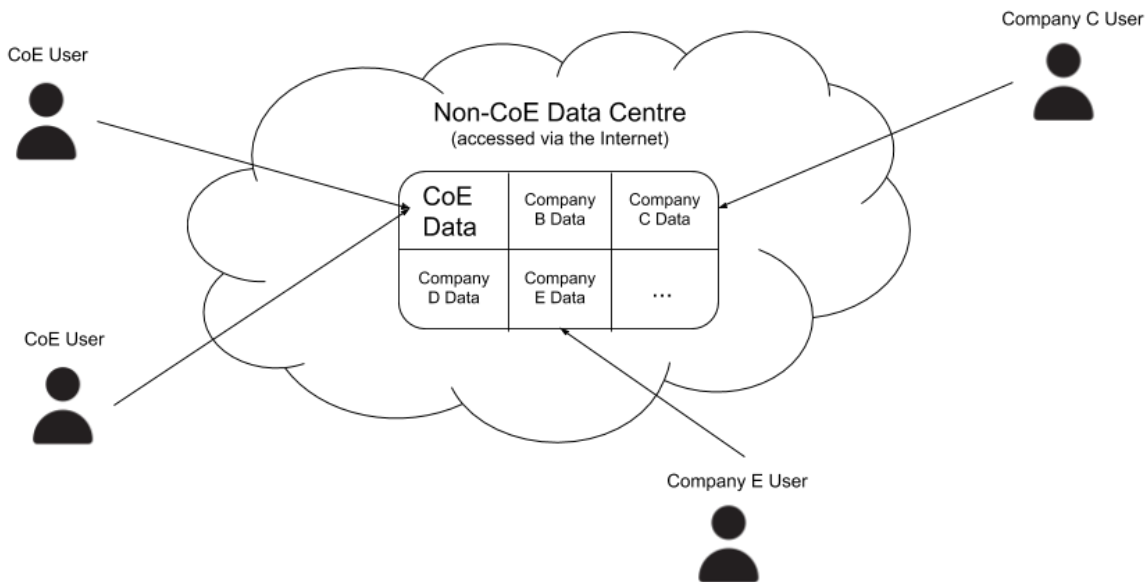
What are the benefits to cloud computing?

Cloud computing can lead to a number of benefits such as reduced need for space, equipment and maintenance – the vendor looks after all of these considerations.

It can also reduce the in-house burden of needing a team of program specialists, database managers and helpdesk agents who deal with ensuring that the applications are up to date and running properly, as these responsibilities are also transferred to the vendor.

By outsourcing to a specialized vendor, there is potential for overall cost savings for the customer (the City), as the vendor can capitalize on economies of scale resulting in lower operating costs than the City would be able to realize operating in-house.

What are the risks related to cloud computing?

As much as there may be a number of benefits, using cloud services introduces new and different risks as well.

Cloud computing can result in an organization losing the ability to control who accesses the facilities where data is stored, and the level of security used to protect those sites.

The organization also relies on the service provider to ensure the ongoing and optimal performance of the application and network. If the service provider's performance fails, the City's information or ability to make use of a potentially critical application could be at risk. As importantly, the City's productivity may suffer due to the impact of network failures that lead to unplanned downtime.

Depending on how the cloud service is designed, organizations using those services may not have as much control over things such as security of data, users' access to services or incident response processes.
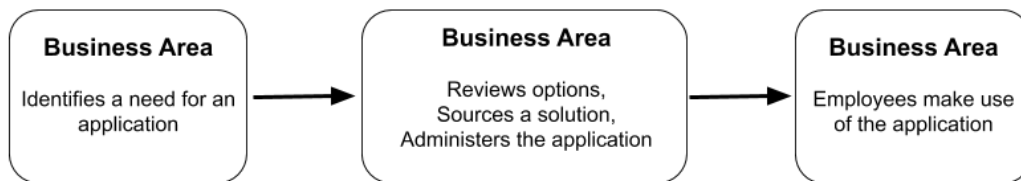
Centralized vs. Decentralized models

Some organizations operate cloud services in a fully *centralized* manner, where one part of the organization has visibility and control over those operations. This model offers the greatest level of control, but generally also carries the highest cost and administrative burden. If the City of Edmonton were to operate in this manner, it would most likely be the Open City and Technology Branch performing that centralized role, and the basic process would be as follows:

Centralized Model

Alternatively, organizations can take a *decentralized* approach, where there is no single group to control cloud services. Individual business areas are able to implement and operate cloud services on their own. A decentralized model presents higher risk if the individual business areas don't follow best practices for implementing cloud services; however, this model provides more operational flexibility to the business areas as they don't require the involvement or approval of another operating group. The basic process flow of a fully decentralized model would be as follows:

Decentralized Model

The City of Edmonton operates in a *hybrid* model with respect to cloud computing; certain cloud services are controlled from a centralized perspective, but the City also allows decentralized operation of cloud services. These decentralized operations are still required to go through an initial review with the Open City & Technology Branch, however given the ease of implementing a cloud service, this may not occur in all instances (whether intentionally or by accidental omission).

Hybrid Model
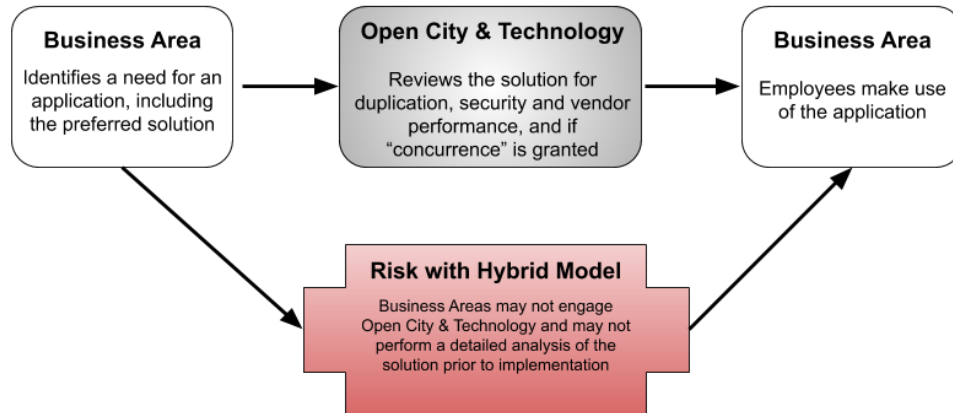
In order to protect the City's digital assets[1], the Open City and Technology Branch has created a governance framework that sets out expectations of any business areas controlling their own services. Part of this includes a requirement for business areas to seek agreement from the Open City and Technology Branch in advance of implementing a new service, which would only be granted after a review of the service.

As long as the governance framework is well-designed, and those employees who are responsible for the services adhere to that framework, operating in a decentralized or hybrid model is generally considered to be acceptable from an organizational risk perspective.

Why was this audit performed?

Given the rapidly changing environment in which IT operations now exist, and the popularization of cloud computing as a model for IT services, we felt that this was an appropriate time to evaluate the governance framework and operation of cloud services in place at the City.

This increase in cloud service usage, combined with the hybrid model in use at the City, means that it is more important than ever to have a strong framework in place and for business areas to adhere to comply with corporate policy.

---

[1] **Digital Asset** - A digital resource that the City possesses or employs and assists in achieving its business objectives. Digital Information, and supporting technology, as well as Operational Technology (such as Health and Safety systems) are examples of digital assets. [*COE Definition*]

Governance

Governance framework for cloud computing

Prior to the Fall of 2018, cloud computing requirements at the City were not fully defined and guidance was provided on an ad hoc basis.

Beginning in 2019, the Corporate Information Security Office within the Open City and Technology Branch began to create and implement formal directives and standards around cyber security, which includes the use of cloud services. They have also published a number of resource documents specifically covering contractual requirements and key controls relating to cloud services.

Collectively, these directives, standards and guiding documents will be referred to as the "governance framework" for cloud computing.

What are the best practices?

Best practices can be viewed as falling into two categories; before a cloud service is put into use (pre-implementation), and once that service is being used (continued operations).

Pre-Implementation

Prior to a cloud service being adopted or implemented, there is a level of due diligence that should be taken into account. For instance:

Is there a specific reason for not using a service that is already in use within the City?

Is the vendor a reputable company with a strong history of operations?

Can the vendor demonstrate that their systems can adequately protect the City's digital assets, in line with the criticality of the service or the sensitivity of information being stored?

Continued Operations

When a cloud service is being used, there are a number of considerations that should also be in place, such as:

Is the City able to control access to the service, and are user accounts reviewed on a regular basis?
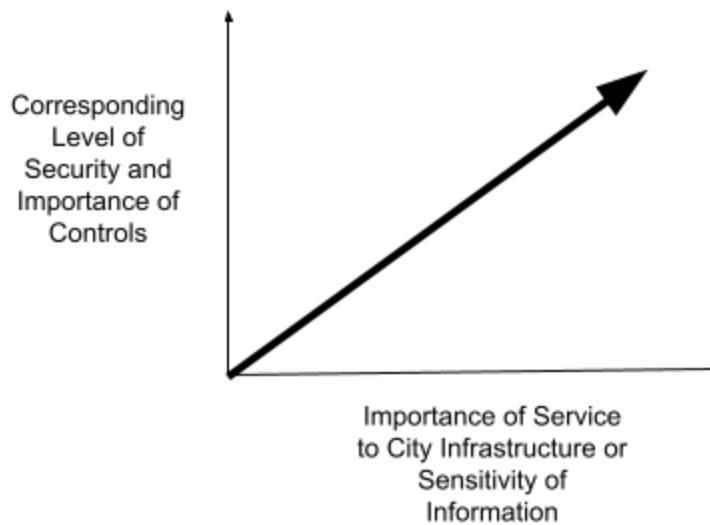
Are the security levels still appropriate for the criticality of the service or the type of information being stored?

Is the performance of the vendor monitored on an ongoing and regular basis?

The amount of due diligence and focus on controls should be in line with the criticality of the business function and the sensitivity of the information stored by the service; that is, if the service relates to things such as critical infrastructure or health and safety, or if it contains private information, more work should be done to ensure that the service is well run by the vendor, appropriate security is in place, and information is adequately protected, as shown in the graphic below.

Corresponding Level of Security and Importance of Controls

Importance of Service to City Infrastructure or Sensitivity of Information

What did we do?

The City of Edmonton's governance framework was designed to align with ISO[2], an established source for best practices in a variety of business processes, including information technology.

ISO published a code of practice specifically related to cloud services[3], which includes implementation guidance over and above their standard information security controls. The City's cloud-related requirements and guidance were reviewed for alignment with ISO's suggested guidance.

Over and above the ISO guidance, the City's governance framework was also compared to Government of Canada guidance[4] for use of cloud services.

This review was performed to determine whether or not the City's governance framework was designed in such a way that additional considerations and risks would also be addressed.

What did we find?

The City's current governance framework aligns with ISO suggested guidance. It addresses several key control activities:

✓ Organization of information security, including definition of roles and responsibilities;

✓ Access to services, controlling who is able to access them and in what capacity;

✓ Security around how the services are operated and maintained; and,

✓ Relationships with suppliers of cloud services, including details of what should be included in the terms and conditions of contractual agreements.

The City's cloud computing governance framework is aligned with the ISO guidance, and is also designed such that it addresses the additional considerations and risk areas that were identified in the Government of Canada guidance.

---

[2] ISO stands for the International Organization for Standardization.
[3] ISO Standard 27017-2015
[4] Government of Canada Security Control Profile for Cloud-based GC Services v1.1, 2018

During our audit, we reviewed the *Software Asset Management Standard Operating Procedure*. This internal procedure outlines the requirement for new software, including cloud services, to go through a review process to ensure that the service is needed (nothing currently used by the City could achieve the same purpose), and that the service is secure. The procedure has not been internally reviewed in over four years, even though it notes that it should be reviewed annually. This document should be updated as necessary, and should continue to be reviewed on a regular basis.

Recommendation 1
Update and review the Software Asset Management SOP

Ensure that the Software Asset Management Standard Operating Procedure is updated and is reviewed on a regular basis

Responsible Party

Branch Manager,
Open CIty & Technology Branch

Accepted by Management

Management Response

The Software Asset Management Standard Operating Procedure will be reviewed, updated and communicated to impacted personnel. The Standards Operating Procedure will be reviewed annually for accuracy and updated as needed.

Implementation Date

March 31, 2021

Awareness of governance framework

The nature of cloud computing makes it easy for a business area, or even an employee within a business area, to start making use of a service without following best practices or corporate policy. In many cases, all that is required is for a user to set up an account and they are able to start using the service.

Testing performed as part of control effectiveness indicated a lack of awareness of the various component parts within the City's governance framework. Branch Managers were made aware of their responsibilities related to services that their business areas were operating in April and May of 2019, and the Cyber Security Administrative Directive was approved in June of 2019. Beginning in 2019, OCT has also held quarterly Cyber Security Advisory Group meetings, with representatives from each City Department, with a mandate to "support the fulfillment of the business and service provider responsibilities as outlined in the Cyber Security Administrative Directive. Even though the cloud services found to be in use were each implemented prior to the formal governance framework, there should be awareness of current requirements.

OCT is positioned to assist business areas with understanding and navigating the requirements of the Directive, but given the hybrid model in use they are not in a position to know how each cloud service is being managed. Given that the City operates in a hybrid manner with respect to cloud services (that is, they allow business areas to make use of the services without centralized control), the accountability and responsibility for use of those services resides with the Branch Managers.

Regular reminders can help Branch Managers be continuously aware of their responsibilities to protect and safeguard the City's digital assets, including use of cloud service and information stored in the cloud.

Recommendation 2

Ensure Branch Managers are reminded of the responsibilities on a regular basis

Ensure that Branch Managers in areas operating cloud services are regularly reminded of their responsibilities under the Cyber Security Administrative Directive.

Responsible Party

Chief Information Security Officer, Open City & Technology Branch

Accepted by Management

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 in 2019, the Administrative Directive was socialized with the Executive Leadership Team and each of the Departmental Leadership Teams. The responsibility for compliance with the Cyber Security Administrative Directive and associated Standards continues to remain with Branches operating cloud-based services and other technologies.

The Corporate Information Security Office will continue to regularly remind Branch Managers of their accountabilities related to cloud-based services, as well as the availability of assistance and guidance from the Open City & Technology Branch as well as the Corporate Information Security Office.

Implementation Date

March 31, 2021

Control Effectiveness

What did we do?

We performed a high level scan of 10 cloud services potentially accessed by the City, of which we identified only two services with continuous use. We performed a detailed review of these two cloud services to determine whether or not they were compliant with the governance framework.

We asked the business area a series of questions to determine why, when and how the decision was made to use the service (pre-implementation due diligence); we also asked a series of questions related to the ongoing use and maintenance of the service, and vendor monitoring.

The two cloud services that were found to be in use related to file sharing, and to customer relationship management. We are not detailing the particular cloud services in use, or the Branches that are using them, as this could expose the City to additional risk.

What did we find?

Even though the amount of testing related to cloud service usage was limited, there are still findings from the work that indicate a lack of compliance with Cyber Security Administrative Directive and the governance framework.

Pre-Implementation

Each instance of use was implemented before the current version of the governance framework was in place; however, there are still principles from the pre-implementation stage that should be evaluated even if the service is currently in use.

For example, it would still be diligent to assess the reason for using the service and to determine whether something else currently in use within the City could accomplish the same purpose; this is especially relevant when there is a cost related to using the service.

It would also be prudent to assess the vendor and whether or not they continue to be a reputable service provider, as part of continued operations of the cloud service.

Neither of the business areas using the file sharing service vetted that use through the Open City and Technology Branch.

Continued Operations

File Sharing Service

Both instances of the file sharing cloud service were implemented in order to share large files with external partners, at the request of those partners.

Information shared by one of the two business areas is considered private and confidential, which increases the need for use of that service to comply with the governance framework.

There are a number of controls that are not being managed, with the use of the file sharing cloud service:

Within one of the business areas, accounts are set up individually, with no ability for someone else in the business area to turn off access. Without being able to control access to the service, if an employee were to leave the City that person could still have access to anything that was stored in the cloud. This contrasts with the City's use of centrally-managed cloud services, where the City is able to turn off a former employee's access.

The business areas are unaware of the security levels in place with the service, and therefore cannot determine if those levels are appropriate for current usage. Reliance is being placed on the external partners having done enough due diligence to ensure that security levels are appropriate.

The business areas are not monitoring vendor performance on a regular basis. This means that they may be unaware if issues exist with the service provider's operations, including issues that could suggest usage should be discontinued.

Customer Relationship Management Service

One business area uses the service as a customer relationship management tool, whereas the other area uses it solely for approving time related to contractor usage. The operational controls around use of the customer relationship management cloud service are stronger than those in place with the file sharing service.

With respect to the controls around the cloud service:

The service provides an ability to centrally control user accounts, which is necessary to be able to regulate access for both current and departing staff.

Risks related to the security of the customer relationship management service are lower based on the nature of its use, but may still contain some confidential information. This requires that the business areas be aware of and comfortable with the security levels in place.

The business areas are not monitoring vendor performance on a regular basis. This means that they may be unaware if issues exist with the service provider's operations, including issues that could suggest usage should be discontinued.

These findings indicate non-compliance with the Cyber Security Administrative Directive and overall governance framework, which is important to maintain continued operations and the security over the City's digital assets. Business areas operating cloud services should comply with the controls included in the framework.

Recommendation 3
Ensure compliance with the Cyber Security Administrative Directive

Ensure that business areas operating the cloud solutions reviewed in this audit are able to demonstrate compliance with the Cyber Security Administrative Directive, or have explicitly accepted the risks of continued operations.

Responsible Party

Branch Manager,
Open CIty & Technology Branch

Accepted by Management

Management Response

The responsibility for compliance with the Cyber Security Administrative Directive and associated Standards continues to remain with Branches operating cloud-based services and other technologies.

The Open City & Technology Branch will request that the business areas highlighted in this audit demonstrate their compliance with the Cyber Security Admininstructive Directive. The Open City & Technology Branch will develop and provide a self-assessment framework to the business areas, for the business areas to perform the self-assessment of compliance. If the business areas have not and do not wish to align to the Cyber Security Administrative Directive, their acceptance of risks will be formalized.

Implementation Date

September 30, 2021

Conclusion

In this audit, we reviewed whether or not the City's cloud computing policies, or governance framework, are in line with best practices and whether there are any control deficiencies that could negatively impact the organization.

Governance

The governance framework in place relating to cloud computing, specifically the Cyber Security Administrative Directive and related standards and resource documents, are aligned with best practices.

One document within the framework was found to be outdated, although still valid, and there is potential for improved communication with business areas relating to awareness of the governing framework. Recommendations were made to address each of these issues.

Control Effectiveness

The cloud services that we reviewed in detail were implemented prior to the governance framework, meaning there was a lower expectation around business areas having followed policies related to pre-implementation controls.

Those services, however, should be complying with the governance framework as it applies to continued operation of the services. We made one recommendation to ensure that operation of the services comply with the framework, or that Branch Managers (as staff accountable for use of the services) have acknowledged and accepted any risks related to non-compliance.

This audit involved participation of staff from a number of areas within Administration, and we thank them for their cooperation

Appendix - Audit Scope

The City does not currently maintain a full listing of all cloud services in use by all of the business areas. As a result, we combined information from multiple sources to try to determine which services were in use.

Due to the way that our population was obtained, there was a limitation on the scope of our audit – we had to use a potentially incomplete population.

From a review of the population and an assessment of potential risks related to each, we selected ten cloud services to perform detailed control testing on.

Cloud Services Reviewed
File Sharing Service 1
File Sharing Service 2
Video Surveillance Service 1
Video Surveillance Service 2
Online Payment Processing Service
Customer Relationship Management Service 1
Customer Relationship Management Service 2
Online Form Building Service
Newsletter Distribution Service
Online Survey Management Service

The City does not currently make use of any specific tools to monitor or control employee use of cloud services, meaning that our determination of potential usage was based on data from logs of internet access, with a focus on web addresses potentially relating to those cloud services.

We reviewed use of cloud services based on potential user access between January 9 and February 7, 2020. Current tools in place only capture 30 days' worth of internet access, meaning that our ability to determine actual user access was also limited. We were further limited by the fact that when users accessed websites via the internal Wi-Fi network, specific user accounts were not logged, meaning that more users could have been accessing cloud solutions than we were aware of.

Our initial high level scan resulted in a number of false positives, meaning many of the cloud services were not actually being used for business purposes. Some of the reasons that these services were initially identified based on user logs, but didn't relate to business use, included:

Some results that were logged related to personal use as opposed to business use;

Websites were accessed for other business purposes (such as performing research), but did not represent cloud service usage;

Logged access could have related to company advertisements running in the background of other sites, without the user being aware; and,

Regarding newsletter distribution and survey management services, access could be related to users receiving newsletters or responding to surveys as opposed to creating and distributing them.

These limitations didn't prevent the completion of the audit, however they did restrict our ability to provide any assurance around the use of cloud computing services as a whole. Testing performed provided indicators of control gaps, but the results of that testing cannot be extrapolated to the entire cloud computing environment.