# Administration Response - Cloud Computing Audit

**Recommendation**

That the February 11, 2021, Financial and Corporate Services report FCS00334, be received for information.

## Executive Summary

The City Auditor's review of access to the City of Edmonton's Cloud Computing was completed January 11, 2021. Administration accepts the Auditor's recommendations to regularly review the Software Asset Management Standard Operating Procedure, to remind Branch Managers of their responsibilities related to, and compliance with, the Cyber Security Administrative Directive.

## Report

Cloud computing allows the City of Edmonton access to a shared pool of computing resources, which are managed by a different organization. Cloud computing allows the Administration to rely less on in-house hardware and expertise, and provides flexibility to different services. Some examples of cloud computing services in use at the City are: the Google suite, Visier, Taleo, and MailChimp. To minimize risks to information security or service interruptions, a strong framework for how and when to use cloud computing services is important.

### Cloud Computing Audit

*Recommendation 1:*
In their review of the City's practices, the Office of the City Auditor found that the governance framework for cyber security and cloud computing was reasonable and based on the industry leading International Organization for Standardization guidance. The auditor also looked at City resources regarding the acquisition of software assets. The auditor found that, while the procedure was valid, it has not been reviewed and updated in four years. It is important to keep guidance up to date to reflect the City's current software and emerging risks.

*Recommendation:*
Update and review the Software Asset Management SOP and 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

*Management Response:* Accepted

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

*Implementation Date:* Q1 2021

*Recommendation 2*:
City Deputy City Managers and Branch Managers were informed of their cyber security responsibilities as Asset Owners during the roll out of the Cyber Security Administrative Directive in 2019 at the Departmental Leadership Meetings. However, the Auditor found that there was limited ongoing awareness of those responsibilities for those leaders, which could be a risk to compliance and information security. The Cyber Security Administrative Directive, rolled out in 2019, addresses the accountabilities of Asset Owners. The Directive is included for information as Attachment 1.

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

*Responsible Party:* Corporate Information Security Officer, Open City & Technology Branch

*Management Response:* Accepted

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:* Q1-2021

*Recommendation 3*:

The Auditor found that some service areas were not in full compliance with the Cyber Security Administrative Directive, in particular a risk to City files or customer information. Risks were more pronounced in systems that predated the Directive.

*Recommendation:*
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

*Management Response:* Accepted
The Open City & Technology Branch will request that the business areas highlighted in this audit demonstrate their compliance with the Cyber Security Administrative 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. The Open City & Technology Branch will review the completed self assessment, however if the business areas have not and do not wish to align to the Cyber Security Administrative Directive, the acceptance of risks will be formalized by the Asset Owner.

*Implementation Date:* Q3 2021

## Corporate Outcomes and Performance Management

| **Corporate Outcome(s): Conditions of success** | | | |
|---|---|---|---|
| **Outcome(s)** | **Measure(s)** | **Result(s)** | **Target(s)** |
| Processes and procedures for cloud application management are communicated and implemented consistently to provide efficient service delivery and safeguard digital assets. | Standard Operating Procedure updated and reviewed annually for currency | A document that is dynamic and up to industry standards as they evolve | 100% by Q2 2021 |
| | Branch Manager awareness performed annually | A memo will be annual distributed to ensure BMs understand their accountabilities and responsibilities | 100% by Q2 2021 |
| | Compliance with the Cyber Security Administrative Directive and Standards | Risks are understood by Asset Owners and/or accepted if non-compli. | 100% by Q3 2021 |

## Attachment

1. Cyber Security Administrative Directive

**Others Reviewing this Report**

- G. Cebryk, Deputy City Manager, City Operations
- R. Smyth, Deputy City Manager, Citizen Services
- B. Andriachuk, City Solicitor