Office of the City Auditor

1200, Scotia Place, Tower 1
10060 Jasper Avenue
Edmonton, Alberta T5J 3R8

edmonton.ca/auditor

Information Technology Disaster Recovery Planning Audit – Redacted Public Report

June 12, 2018

The Office of the City Auditor conducted this project in accordance with the *International Standards for the Professional Practice of Internal Auditing*

Information Technology Disaster Recovery Planning Audit

Table of Contents

1 Introduction 1
2 Background 2
3 Audit Objective, Scope and Methodology 3
4 Observations and Recommendations 4
4.1 Program and Components are Developed, Maintained and Tested 5
4.2 Third-Party Service Provider, Backups, and Data Centres 7
5 Conclusions 9

This page is intentionally blank.

Information Technology Disaster Recovery Planning Audit

1 Introduction

Information Technology (IT) systems are relied upon by every area of the City's operations. Without reliable access to those systems, City operations would be severely impacted. In order to prepare for a potential large scale loss of IT systems, the Open City and Technology Branch has implemented a disaster recovery program, which notes that:

> Because IT is susceptible to outages, including large scale disasters, the City must ensure sufficient preparedness. IT Disaster Recovery planning is important because it provides assurance that the City is prepared for and will respond with appropriate urgency to incidents and disruptions to critical business services.

The Office of the City Auditor (OCA) 2017 Annual Work Plan included an audit of IT Disaster Recovery Planning, to assess the Branch's preparedness in the event of an unforeseen service disruption at the City of Edmonton.

This report is the redacted, publicly available version; we removed portions of this report as they are considered exempted information under Sections 20 (disclosure harmful to law enforcement), 24 (advice from officials) and 25 (disclosure harmful to economic and other interests of a public body) of the Freedom of Information and Protection of Privacy Act. Consequently, the full report is available only to authorized individuals.

2 Background

The Open City and Technology Branch (the Branch) is responsible for providing IT services to the City's departments and branches. This technology includes networks, databases, servers, internet connections, email, and software applications.

The Branch maintains more than 140 business applications and 5 enterprise-wide applications. They also maintain over 300 network and wireless sites, 15,000 devices and 1,500 computer servers. A recent business impact assessment resulted in users and stakeholders identifying a total of 576 applications that are used for City operations. For each of those applications, users identified their expectations with respect to how quickly they would need their services recovered in the event of an outage and the maximum acceptable level of data loss.

The potential loss of services due to an interruption in information technology necessitates the preparation, implementation, and maintenance of a comprehensive IT disaster recovery program. The Branch has an IT Disaster Recovery Program (the Program) that is intended to plan for how the City would recover technology-based operations after a human-induced, technological, or natural disaster, within targeted timelines.

One 2017 survey by a research and advisory firm indicated that approximately 80 percent of survey respondents experienced at least one incident in the preceding two years, which required an IT Disaster Recovery Plan.

In order to update its overall disaster recovery preparedness, the Branch hired consultants to perform an external assessment and to coordinate with all of the business areas in the City to determine their IT needs. The IT Disaster Recovery Program was one of the deliverables from the consultants.

It is important to note that while the Branch is responsible for providing IT services and processes related to recovering in the event of a disaster, the expectations around recovery times and the resources dedicated to maintain those service levels should be approved at a more senior, Corporate level.

Disaster recovery preparedness requires complex and resource-intensive efforts. The majority of City of Edmonton critical IT applications are operated from a primary data centre, with a secondary data centre available and intended to support business services in a disaster event.

When operation of an application is transferred from the primary site to a secondary site or backup site, this can be fully automated, partially automated but requiring some human intervention, or a fully manual process. Generally speaking, the more automated the process is the quicker the recovery will be, but the greater the costs will be as well.

3 Audit Objective, Scope and Methodology

Audit Objective

The audit objective for this audit was to evaluate the City's IT disaster recovery preparedness in the event of a process disruption.

Audit Scope

Our audit focused on the effectiveness of the Program and its components. In performing that work we also reviewed other controls that would support the ability to resume IT operations if faced with the loss of the primary data centre.

Within the context of this audit, we refer to a disaster as being any incident that removes the ability of the City to operate from the primary data centre. This could be the result of anything from a fire or flood to loss of power, or the result of specific actions by a person with malicious intent. Although this audit focused on disaster recovery preparedness at a large-scale level, as opposed to being able to recover from loss of individual applications, the ability to recover critical applications individually would need to be able to take place as part of the fulsome disaster recovery response.

Methodology

In order to achieve our audit objective we:

- Interviewed staff responsible for disaster recovery preparedness.
- Reviewed industry best practices related to IT disaster recovery preparedness.
- Evaluated the effectiveness of controls and requirements within the Program.

For the purpose of determining best practices as they relate to our audit, we referred to guidance issued by the Information Systems Audit and Control Association (ISACA), which is an internationally-recognized association with a focus on IT governance.

4 Observations and Recommendations

To evaluate the City's IT disaster recovery preparedness we reviewed:

1. The IT Disaster Recovery Program and supporting plans to ensure they are developed, maintained and tested.
2. The roles, responsibilities and expectations of third-party (service) provider agreements to ensure they are clearly defined and monitored.
3. The requirements and procedures for backups and storage.
4. The data centres to ensure they are designed and managed to protect equipment and personnel.

Overall, we found that the City can improve its disaster recovery preparedness. While the Branch has designed a Disaster Recovery Program that aligns with best practices, it has not implemented all the component parts of that Program.

20(1)(m), 24(1)(a), 25(1)(c)

4.1 Program and Components are Developed, Maintained and Tested

We reviewed the IT Disaster Recovery Program and supporting technical recovery plans to determine if they were designed in alignment with best practices (*conceptually, does the Program take the specific best practices into account?*), and then determined whether or not those components were effective (*are those components in place and working as designed?*).

20(1)(m), 24(1)(a), 25(1)(c)

We found that the Program is well-designed, as it contains the components that we were looking for and aligns with best practices. The Program represents a formalized approach to disaster recovery planning.

Our testing identified some components of the Program that have not yet been fully implemented. Specific details of our findings were removed pursuant to *Freedom of Information and Protection of Privacy Act* exemptions discussed in the report introduction.

20(1)(m), 24(1)(a), 25(1)(c)

Ensuring that all components of the Program are in place will demonstrate that it is effective, and that the City is able to respond to a disaster that removes the ability to operate from the primary data centre. In addition it would also be beneficial for the current Branch Manager to formally approve the Program to show that it still meets the needs and operational direction of the Branch.

Recommendation 1 – Fully Implement the Disaster Recovery Program

We recommend that the Branch Manager, Open City and Technology, approve the IT Disaster Recovery Program and ensure the Branch has fully implemented all the component parts of the Program. This will ensure that the Branch can demonstrate the effectiveness of the Program.

Management Response and Action Plan

Accepted

Action Plan: The IT Disaster Recovery Program was approved in September/October of 2017 and was reviewed and approved by the Current Branch Manager of Open City and Technology in December of 2017. Administration agrees with the audit recommendation and will ensure the implementation is completed by Q4 2021.

Information Technology Risks requiring Corporate awareness are reported to the Executive Leadership Team on a quarterly basis. Progress on the implementation of this recommendation will be presented along with the quarterly risk report.

Planned Implementation Date: Q4 2021

Responsible Party: Branch Manager, Open City and Technology

4.2 Third-Party Service Provider, Backups, and Data Centres

We reviewed and documented the use of a third-party service provider, backup and offsite storage processes, and the controls in place at the primary and secondary data centres.

Third-Party Service Provider

The City currently uses a third-party to provide a facility for the secondary data centre. We reviewed the contract with the supplier and the services they provide, to ensure that the City is not exposed to significant risks.

The only risk that we found related to using the third-party supplier is that there is some question as to whether or not the supplier will be able to continue providing facility services.

Backups

We documented the backup and storage processes which would support the ability to transfer operations to a secondary data centre and recover from a disaster.

Data Centres

We reviewed both the primary and secondary data centres to ensure that the Branch has designed and managed them to protect equipment and personnel. We reviewed locations, physical access and security controls, monitoring, power supplies, environmental sensors, and fire suppression systems.

We found that both data centres are controlled by multiple levels of security, to ensure that only authorized individuals are on site. Power supplies at each location have built-in redundancies, as well as backup generators. Environmental sensors are in place and tested, to ensure that conditions such as temperature and humidity are appropriately controlled, and fire suppressions systems are installed.

20(1)(m), 24(1)(a), 25(1)(c)

Backup and offsite data storage processes are in place, and data centres were found to be designed to protect equipment and personnel. Additional discussion and findings related to this section were removed pursuant to *Freedom of Information and Protection of Privacy Act* exemptions discussed in the report introduction.

Recommendation 2 – In Private

One recommendation was removed pursuant to *Freedom of Information and Protection of Privacy Act* exemptions.

Management Response and Action Plan

Accepted

Action Plan: Administration agrees with this audit recommendation and will ensure the implementation is completed by Q2 2019.

Further details of the Management Response and Action Plan were removed pursuant to *Freedom of Information and Protection of Privacy Act* exemptions.

Planned Implementation Date: Q2 2019

Responsible Party: Branch Manager, Open City and Technology

5 Conclusions

Overall, we found that the City can improve its disaster recovery preparedness.

The Branch has designed an IT Disaster Recovery Program that is aligned with best practices, but additional work is required in order to be able to demonstrate the effectiveness of the program. 20(1)(m), 24(1)(a), 25(1)(c)

We made one recommendation to ensure the effectiveness of the Program.

We also found that there is a potential risk in using a third-party supplier for the secondary data centre, in that the supplier could potentially end that relationship, which the Branch is currently aware of. Backup and offsite data storage processes are in place, and both the primary and secondary data centres were found to be designed to protect equipment and personnel. 20(1)(m), 24(1)(a), 25(1)(c)

One additional recommendation was made in private.

We thank the staff and management of the Open City and Technology Branch, and others who assisted us in completing this project.