Chapter 14
Central Services—Securing the Data Centre

1.0 Main Points

The Ministry of Central Services provides IT services to 18 government ministries and seven other agencies. The Ministry uses a data centre, operated by a third-party service provider, to deliver IT services to its clients on its behalf. The data centre houses computer network equipment and servers that support client systems and data.

At December 2018, the Ministry addressed one of our two remaining recommendations related to securing the data centre.

We found the Ministry holds an adequate agreement with its service provider to offer disaster recovery services to the Ministry's clients. Disaster recovery plans for critical client IT systems are tested annually. Disaster recovery plans help clients recover as quickly as possible and continue to provide key services in the event of a disaster.

The Ministry has made progress on properly configuring and updating its server and network equipment, using a risk-based approach. The Ministry properly configures new servers and monitors the configuration of all servers. Network equipment is up-to-date. However, the data centre's firewall rules do not sufficiently restrict access to the data centre. Inadequate firewall rules increase the risk of a security breach.

2.0 Introduction

2.1 Background

The former Information Technology Office implemented an IT data centre in May 2005. In December 2010, the Information Technology Office outsourced the data centre to a third-party service provider. Effective May 25, 2012, the Information Technology Office became part of the Ministry of Central Services. The Ministry continues to outsource the data centre to a third-party service provider.

See **Section 4.0** for a listing of the ministries and agencies using the data centre to house their systems and process their data, which the Ministry refers to as clients.

2.2 Focus of Follow-Up Audit

Our *2006 Report – Volume 3*, Chapter 6, reports the results of our first audit on whether the former Information Technology Office provided adequate controls to protect the confidentiality, integrity, and availability of client IT systems and data. From 2006 to 2015, we audited the data centre annually. Given progress in making improvements, we decided to do follow-up audits every two to three years.

We last reported on the Ministry's controls to secure the data centre in our *2016 Report – Volume 1*, Chapter 5. We found two outstanding recommendations remained; the Ministry needed to:

- Adequately configure and update its server and network equipment
- Have a complete, and tested, disaster recovery plan for the data centre and clients' systems

This chapter describes our follow-up of management's actions on the two outstanding recommendations.

To conduct this audit engagement, we followed the standards for assurance engagements published in the *CPA Canada Handbook – Assurance* (CSAE 3001). To evaluate the Ministry's progress toward meeting our recommendations, we used the relevant criteria from the original audit. Management agreed with the criteria in the original audit.

We reviewed the Ministry's completed disaster recovery plans and testing conducted on the plans. Additionally, we assessed the configuration of the data center's firewalls, reviewed the Ministry's data classification policy, and assessed the Ministry's process to apply timely updates to servers and network devices.

3.0 Status of Recommendations

This section sets out each recommendation including the date on which the Standing Committee on Public Accounts agreed to the recommendation, the status of the recommendation on December 31, 2018, and the Ministry's actions up to that date.

3.1 Disaster Recovery Plans in Place and Tested

> ***We recommended the Ministry of Central Services have a disaster recovery plan for the data centre and client systems.*** (*2006 Report – Volume 3*, p. 216, Recommendation 4; Public Accounts Committee agreement April 3, 2007)
>
> **Status** – Implemented

The Ministry established disaster recovery plans and testing for critical client IT systems and data.

The Ministry renewed the data centre agreement with its service provider in 2016. Under the agreement, the Ministry receives disaster recovery testing once a year for four clients' critical IT systems.[1,2] The agreement allows for additional disaster recovery testing as the Ministry determines it needs.

[1] The four clients include the Ministry of Social Services, Ministry of Finance, Ministry of Justice, and Ministry of Advanced Education. A few of the Ministry's clients also have separate disaster recovery agreements with other service providers to restore critical IT systems and data if a disaster occurs (e.g., Ministry of Finance – tax system; Ministry of Economy – oil and gas revenue system)

[2] Critical IT systems include the correctional and justice information system, student loan system, MIDAS financial and payroll system, child case management system, and the Saskatchewan Housing Corporation financial system.

Disaster recovery testing takes place in May or November each year. The service provider works with the Ministry and the applicable clients to recover the critical IT system with connectivity to the service provider's data centre in Ontario. Such a recovery scenario addresses a disaster where the data centre was no longer operational in Saskatchewan.

In addition, the Ministry's data centre service provider now has real-time data backup systems (i.e., redundant backups). This increases data reliability and uptime; there is no longer a need to wait to have a backup restored.

Having disaster recovery plans in place increases the likelihood of critical IT systems that support key services being available to the Government and the people of Saskatchewan in the event of a disaster.

3.2 Firewalls Not Effectively Configured

We recommended the Ministry of Central Services adequately configure and update its server and network equipment to protect them from security threats. (*2012 Report – Volume 2*, p. 224, Recommendation 2; Public Accounts Committee agreement September 23, 2014)

Status – Implemented, except for Firewall Configuration

Network Devices Updated but Data Centre Firewall Improperly Configured

Central Services uses network devices (e.g., routers, switches, and firewalls) to help protect its data centre from hackers. As of December 2018, we found the network devices are up-to-date and supported.

The Ministry's data centre firewalls are located at appropriate locations, and monitor and report security events. In 2017, the Ministry upgraded the data centre firewalls. Moreover, the Ministry's service provider applies updates to the firewall regularly.

However, we found that the data centre firewalls are improperly configured. The data centre firewalls do not have firewall rules appropriately defined to prevent unwanted access to the data centre. The Ministry is working with its service provider to review and update the data centre's firewall rules.

Inadequate firewall rules increase the risk of a security breach.

1. **We recommend the Ministry of Central Services work with its service provider to configure its data centre firewalls to restrict inappropriate access.**

Servers Receiving Timely Updates

In 2017, the Ministry's service provider conducted a risk assessment to determine a reasonable patching schedule for servers. This schedule ranged from monthly to annually, depending on when server patches become available for each type of server. For 12 servers we tested, the Ministry's service provider applied all known updates to the servers in a timely manner.

The Ministry acknowledges there continues to be unsupported servers, which it manages on behalf of clients that use unsupported applications requiring unsupported versions of operating software. At December 2018, there remains 81 unsupported servers out of 986 servers (100 out of 1000 servers at December 2015). Using unsupported software means security updates (e.g., Windows updates or patches) are not available for these servers, which increases the risk of security breaches and availability issues.

The Ministry communicates to its clients the risks associated with continuing to use unsupported applications that rely on unsupported servers. The Ministry requires its clients to accept the risk of utilizing unsupported applications, or commit to a plan to upgrade the applications to a supported level.

Servers Properly Configured

In 2018, we found the Ministry completed documenting what client data resides on which particular server.

Also, in 2018, the Ministry defined four levels of data classification through their security policies. All new systems and servers added to the Ministry's data centre require the client to assess the level of security required based on data classification. We found the Ministry's Information Security Division conducts a threat risk assessment to determine the security configurations required to build the server securely. Before adding the server to the Ministry's data centre, a scan of the server is performed to ensure the security configuration is appropriate.

Additionally, we found the Ministry's Information Security Division scans all servers monthly, to identify security weaknesses (e.g., improper configurations). The Information Security Division makes change requests to address weaknesses found.

4.0 List of Clients At December 2018

Ministries:

Ministry of Advanced Education
Ministry of Agriculture
Ministry of Central Services
Ministry of Corrections and Policing
Ministry of Education
Ministry of Energy and Resources
Ministry of Environment
Executive Council
Ministry of Finance
Ministry of Government Relations
Ministry of Highways and Infrastructure
Ministry of Immigration and Career Training
Ministry of Justice and Attorney General
Ministry of Labour Relations and Workplace Safety
Ministry of Parks, Culture, and Sport
Public Service Commission
Ministry of Social Services
Ministry of Trade and Export Development

Agencies:

Apprenticeship and Trade Certification Commission
Financial and Consumer Affairs Authority of Saskatchewan
Global Transportation Hub Authority
Saskatchewan Crop Insurance Corporation
Saskatchewan Housing Corporation
Saskatchewan Municipal Board
SaskBuilds Corporation