Chapter 19
SaskBuilds and Procurement—Securing the Data Centre

1.0 Main Points

The Ministry of SaskBuilds and Procurement provides IT services to its clients—government ministries and other government agencies. The Ministry utilizes a data centre that houses computer network equipment and servers to support client systems and data. The Ministry contracts a service provider to deliver these IT services and operate the data centre. Firewalls are in place to prevent unwanted access to the data centre.

As of December 2024, the Ministry worked with its service provider to properly configure its data centre firewalls to restrict inappropriate access to the data centre. It implemented a process to identify higher risk firewall rules using a digital tool (i.e., firewall analyzer). The Ministry reviewed higher risk rules the analyzer identified to ensure they are properly configured to restrict inappropriate access. As a result, the Ministry reduced the number of high and critical risk rules from 87 (as of December 2022) to six by February 2025. Appropriately configuring firewalls help prevent unauthorized access attempts and potential security breaches.

2.0 Introduction

The Ministry of SaskBuilds and Procurement provides IT services to government ministries and agencies using a data centre.[1] Since 2010, the Ministry outsourced the data centre to a service provider.

See **Section 4.0** for a list of ministries and agencies (i.e., clients) using the data centre for their IT systems and data as of December 2024.

2.1 Focus of Follow-Up Audit

This chapter describes our third follow-up audit of management's actions on the one outstanding recommendation related to configuring the data centre firewalls we originally made in 2019.

We concluded the Ministry of SaskBuilds and Procurement had effective processes, except for the area of our one recommendation, to provide adequate controls to protect the confidentiality, integrity, and availability of client IT systems and data.[2] By December 2022, the Ministry partially implemented the recommendation.[3]

[1] The IT data centre for government ministries was implemented in May 2005.
[2] *2019 Report – Volume 1*, Chapter 14, pp. 217–220.
[3] *2021 Report – Volume 1*, Chapter 26, pp. 271–272 and *2023 Report – Volume 1*, Chapter 24, pp. 223–225.

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 recommendation, we used the relevant criteria from the original audit. Ministry management agreed with the criteria in the original audit.

To carry out our follow-up audit, we assessed the configuration of the data centre's firewall analyzer tool and reviewed the Ministry's process to update firewall rules. We used an independent consultant with subject matter expertise to help us assess the Ministry's processes.

3.0 STATUS OF RECOMMENDATION

This section sets out the recommendation including the date on which the Standing Committee on Public Accounts agreed to the recommendation, the status of the recommendation at December 31, 2024, and the Ministry of SaskBuilds and Procurement's actions up to that date.

3.1 Firewall Rules Reviewed and Remediated

> ***We recommended the Ministry of SaskBuilds and Procurement work with its service provider to configure its data centre firewalls to restrict inappropriate access.*** (*2019 Report – Volume 1,* p. 219, Recommendation 1; Public Accounts Committee agreement February 26, 2020)
>
> **Status**—Implemented

The Ministry of SaskBuilds and Procurement implemented a formal process to review and evaluate firewall rules on a regular basis, and to take action on firewall rules posing significant risks to the data centre environment.

The Ministry used a firewall analyzer (an IT tool) up to February 2025 to continually track and monitor its data centre firewall rules. The analyzer assessed which firewall rules are higher risk or may cause vulnerabilities. We found the Ministry reviewed the rules identified by the analyzer on a bi-weekly basis. In February 2025, the Ministry's firewall analyzer vendor went out of business and Ministry management indicated it was looking into a replacement tool.

Since our last follow-up audit, we found the Ministry extensively cleaned up its firewall rules—as of February 2025, only six high and critical risk rules remained that had not been remediated (previously 87 rules). These rules related to one application only and the Ministry planned to remediate these rules in July 2025.

Having appropriately defined firewall rules decrease vulnerabilities and reduce the risk of unwanted access to the data centre.

4.0 List of Clients as of December 2024

Ministries:

Executive Council
Ministry of Advanced Education
Ministry of Agriculture
Ministry of Corrections, Policing and Public Safety
Ministry of Education
Ministry of Energy and Resources
Ministry of Environment
Ministry of Finance
Ministry of Government Relations
Ministry of Highways
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
Ministry of SaskBuilds and Procurement
Ministry of Social Services
Ministry of Trade and Export Development
Public Service Commission

Agencies:

Apprenticeship and Trade Certification Commission
Financial and Consumer Affairs Authority of Saskatchewan
Global Transportation Hub Authority
Provincial Capital Commission
Public Guardian and Trustee of Saskatchewan
Saskatchewan Housing Corporation
Saskatchewan Legal Aid Commission
Saskatchewan Liquor and Gaming Authority
Saskatchewan Municipal Board
Water Security Agency