Chapter 24
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 supporting 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 2022, the Ministry was still working with its service provider to properly configure its data centre firewalls to restrict inappropriate access by updating the firewall rules to safeguard the network. Inadequate firewall configuration and inappropriately defined firewall rules increases the risk of a security breach. The Ministry still has about 87 high risk and critical firewall rules to analyze and address.

2.0 INTRODUCTION

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

See **Section 4.0** for a listing of the ministries and agencies (i.e., clients) using the data centre for their IT systems and data at December 2022.

2.1 Focus of Follow-Up Audit

This chapter describes our second follow-up audit of management's actions on the one outstanding recommendation related to configuring the data centre firewalls we made in our *2019 Report – Volume 1*, Chapter 14.[2]

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 firewalls and reviewed the Ministry's process to update firewall rules.

[1] The IT data centre for government ministries was implemented in May 2005.
[2] *2019 Report – Volume 1*, Chapter 14, pp. 217–220.

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, 2022, and the Ministry's actions up to that date.

3.1 Updating of Firewall Configuration Ongoing

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—Partially Implemented

The Ministry of SaskBuilds and Procurement has progressed in updating its data centre's firewall rules. Firewall rules are the access control mechanism used by firewalls to safeguard a network from harmful applications and unauthorized access. The Ministry still has about 87 high risk and critical firewall rules to analyze and address.

By December 2022, the Ministry implemented a firewall analyzer to continually track and monitor firewall rules.[3] It also developed Firewall Analyzer Procedures for tracking firewall rule changes and insecure firewall remediation. The analyzer has tracked firewall changes since August 2022, and will do so going forward. It also detects insecure firewall rules (i.e., rules that do not align with security requirements).

The Ministry also implemented a process to manually assess the firewall rules which existed prior to August 2022. It reviews approximately 200 rules on a bi-weekly basis. It is focused on reviewing and updating those firewall rules it determined as posing the greatest risk to client data and systems.

At December 2022, management indicated it had updated the high risk and critical firewall rules that had no impact on business operations. The Ministry continues to address the remaining 87 high risk and critical firewall rules. Once this is completed, the Ministry plans to address its less risky firewall rules. At December 2022, the Ministry has about 450 less risky firewall rules to assess. The Ministry expects to be done this work by 2024–25.

We found the Ministry updated about 140 of its data centre's existing firewall rules in 2022 however, it rolled back some of the changes due to unforeseen impacts on clients (e.g., caused issues with cheque printing).

We assessed firewall rules that had not been updated and found a number of firewall rules that are overly permissive (i.e., the rule may allow more access than required for the service or application to properly function). For example, one firewall rule exception allows clear text transmission, which increases the risk that a user's credentials could be obtained. The Cybersecurity Risk Management Branch within the Ministry of SaskBuilds and

[3] Analyzing and updating firewall rules is an ongoing process. The analysis process includes, but is not limited to, identification of firewall rules exceptions and assessment of what services are impacted by the rule, the purpose of the rule, the risk associated with the rule, and the decision made on the rule (e.g., firewall rule removed, further analysis required after assessment).

Procurement identified the risk, communicated it to the client, and the client accepted the risk and implemented mitigating controls (i.e., use of secure transfer protocol for sensitive and confidential information). The client has yet to implement a risk response plan to eliminate the risk completely.

The Ministry continues to work with its service provider, and clients, to address firewall rules and the associated risks.

Having inappropriately defined firewall rules increases the risk of unwanted access to the data centre (e.g., security breach).[4]

4.0 List of Clients as of December 2022

Ministries

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
Executive Council
Public Service Commission

Agencies

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

[4] The Ministry uses a risk-based approach to maintain the security of its data centre network, and implemented a number of other changes (e.g., endpoint protection) in addition to updating firewall rules to help reduce its overall risk of a network security breach.