Status Update

PAC Date January 22, 2025

Chapter 24, SaskBuilds and Procurement – Securing the Data Centre, 2023 Report – Volume 1

Recommendation and Status at Time of Audit	Page	Current Status	Actions Taken to Implement Since PA Report	Planned Actions for Implementation	Timeline for Implementation
Outstanding: 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)*	224	Implemented	The Ministry of SaskBuilds and Procurement reviewed and cleaned up all high risk and obsolete rules on our core firewalls. In addition, the ministry has invested in several compensating controls, which include firewall analysis, enhanced monitoring and detection, and the establishment of a formal process for managing our firewall rules.	N/A – implemented	N/A

Status Update

PAC Date January 22, 2025

Chapter 7, SaskBuilds and Procurement – Responding to Cyberattacks, 2024 Report, Volume 1

Recommendation and Status at Time of Audit	Page	Current Status	Actions Taken to Implement Since PA Report	Planned Actions for Implementation	Timeline for Implementation
New: 1. We recommend the Ministry of SaskBuilds and Procurement centrally and continuously monitor all event logs to identify potential cyberattacks.	133	Implemented	The Ministry of SaskBuilds and Procurement now uses a risk-oriented strategy for event surveillance, utilizing a centralized system for logging and ongoing scrutiny of all mission-critical logs and high risk logs. This strategy is adopted due to the economic impracticality of maintaining constant monitoring across all events.	N/A – implemented	N/A
New: 2. We recommend the Ministry of SaskBuilds and Procurement undertake penetration testing on a periodic basis to identify and address cybersecurity threats.	135	Implemented	The Ministry of SaskBuilds and Procurement has established an in-house team to conduct penetration testing. This testing will be carried out on all new high-risk systems. Additionally, penetration testing for existing systems will be guided by two primary considerations: the risk level associated with the system and the status of vulnerability assessments.	N/A – implemented	N/A
New: 3. We recommend the Ministry of SaskBuilds and Procurement expand its testing techniques and continuously test its cyber incident response plans.	136	Partially Implemented	The Ministry of SaskBuilds and Procurement has developed an incident response plan and playbooks specifically tailored for critical cybersecurity incidents. These plans outline the necessary steps to effectively manage and mitigate high-risk situations. The ministry prioritizes testing the highest risk scenarios first.	The ministry is currently employing checklists and tabletop exercises, and is exploring the benefits of other testing techniques to achieve this efficiently.	August 1, 2025