Chapter 45
SaskPower—Managing the Risk of Cyber Incidents

1.0 Main Points

SaskPower fully implemented a recommendation from our 2015 audit about managing the risk of cyber incidents. It annually updates its cyber risks assessment and confirms its strategies address those risks.

By confirming its strategies address significant threats of cyber incidents, SaskPower reduces the risk of a cyber attack jeopardizing its ability to deliver power. Depending on the timing and extent of a security incident, disruptions in power may damage power-generating plants and/or transmission equipment, adversely impact businesses in need of power, or put public safety at risk.

2.0 Introduction

SaskPower is the principal supplier of electricity in Saskatchewan operating under the mandate and authority of *The Power Corporation Act*. Its mission is to ensure reliable, sustainable, and cost-effective power for its customers and the communities it serves.[1] It is responsible for serving more than 538,000 customers in Saskatchewan.[2]

This is our second follow-up audit of one recommendation first made in 2015.

Our *2015 Report – Volume 1*, Chapter 18, reports, for the 12-month period ended February 28, 2015, SaskPower had effective processes to manage the risk of cyber incidents for the protection of the provision of power other than the areas reflected in our three recommendations.[3] By August 2017, SaskPower implemented two of our three recommendations.

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

We examined SaskPower's IT risk registers, reports on IT projects, and other relevant documentation. We also interviewed staff responsible for monitoring and responding to cyber incidents.

[1] SaskPower, *SaskPower 2018–19 Annual Report*, p. 12.
[2] SaskPower, *SaskPower 2018–19 Annual Report*.
[3] The original report regarding these recommendations is at www.auditor.sk.ca under the 'Publications' tab, 'Public Reports.' We reported the original audit work in *2015 Report – Volume 1*, Chapter 18, pp. 227–233. auditor.sk.ca/pub/publications/public_reports/2015/Volume_1/18_SaskPower-Cyber%20Incidents.pdf.

3.0 STATUS OF RECOMMENDATION

This section sets out the recommendation including the date on which the Standing Committee on Crown and Central Agencies agreed to the recommendation, the status of the recommendation on August 21, 2019, and SaskPower's actions up to that date. We found it implemented the recommendation.

3.1 Cyber Risk Mitigation Strategy Confirmed

We recommended SaskPower confirm that its cyber risk mitigation strategy addresses the significant threats of cyber incidents that would adversely impact its ability to provide power. (*2015 Report – Volume 1*, p. 231, Recommendation 2; Crown and Central Agencies Committee agreement December 13, 2016)

Status—Implemented

SaskPower annually updates its cyber risks assessment, and confirms its strategies address those risks.

Since August 2017 (our last follow-up audit), SaskPower implemented a number of new strategies to reduce risks it identified in its 2017 risk register. For example, it implemented tools allowing it to better analyze data and identify potential cyberattacks. In addition, it implemented processes to identify and prevent inappropriate sharing of sensitive information. At August 2019, SaskPower was implementing a number of additional strategies to further reduce its risks.

In addition, SaskPower actively monitored attempted security attacks to help assess the effectiveness of its risk mitigation strategies. It reported these results to its Board and executive management.