Chapter 43
Saskatchewan Indian Gaming Authority Inc.— Information Technology Threat and Risk Assessment

1.0 Main Points

The Saskatchewan Indian Gaming Authority Inc. (SIGA) uses IT extensively to carry out its business.[1]

By October 5, 2016, SIGA had implemented all four recommendations we first made in our 2012 audit of its IT threat and risk assessment processes. SIGA has approved an IT risk assessment policy, assessed its IT risks, developed responses to those risks, reported its risk assessment to senior management, and monitored its risks. These improved processes help SIGA understand its IT risks and sufficiently plan to respond to them to keep its IT systems available and secure.

2.0 Introduction

This chapter describes our second follow-up[2] of management's actions on the recommendations we made in our *2012 Report – Volume 2,* Chapter 35, related to SIGA's IT threat and risk assessment processes.

To conduct this review engagement, we followed the standards for assurance engagements published in the *CPA Canada Handbook – Assurance*. To evaluate SIGA's progress towards meeting our recommendations, we used the relevant criteria from the 2012 audit. SIGA's management agreed with the criteria in the 2012 audit. We discussed the key actions taken with management and reviewed supporting documentation.

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 at October 5, 2016, and SIGA's actions up to that date. We found that SIGA had implemented all four recommendations.

[1] SIGA operates six First Nations casinos in Saskatchewan.
[2] We last followed up on management's actions in 2014.

3.1 IT Risk Assessment Policy Approved

We recommended that the Saskatchewan Indian Gaming Authority fully document and approve its plan for assessing the risks to its business from vulnerabilities to its information technology systems. (2012 Report – Volume 2; Public Accounts Committee agreement December 9, 2013)

Status – Implemented

We expected SIGA's IT risk assessment plan to include timelines, expected participants, scope, and planned steps. We also expected the plan would be approved by management.

By October 2016, SIGA's IT Policy Review Committee[3] had approved an IT risk assessment policy. The IT risk assessment policy:

- Included a timeline to complete risk assessments (e.g., upon initial acquisition of a new IT system or when a significant change is made)
- Assigned responsibility to its Senior Vice-President of Information Technology to monitor compliance with policy
- Defined the scope of information systems and information system components that require risk assessment (e.g., infrastructure hardware and application software, including cloud-based applications)
- Provided detailed guidelines for completing its IT risk assessment (e.g., identify and document potential threats and vulnerabilities, estimate the likelihood each vulnerability will occur, estimate each vulnerability's impact on operations, etc.)

3.2 IT Risk Assessment Complete

We recommended that the Saskatchewan Indian Gaming Authority follow its policies by documenting its analysis of the impact and likelihood for information technology risks and developing responses for significant risks. (2012 Report – Volume 2; Public Accounts Committee agreement December 9, 2013)

Status – Implemented

Since 2014, SIGA followed its policy and documented its IT risk assessment in an IT risk register. SIGA's IT risk register includes analysis of the impact and likelihood for IT risks it faces, the planned responses to the identified risks, and the estimated residual risks that require further action or acceptance.

[3] SIGA's IT Policy Review Committee consists of the: Vice President of IT of Business Development, Director of IT (Infrastructure), Director of Security and Quality Assurance, Director of Business Applications, and Manager of Technical Services.

3.3 IT Risk Assessment Results Reported to Senior Management

We recommended that the Saskatchewan Indian Gaming Authority report to senior management:

- The impact of significant information technology risks
- Responses taken for those risks
- The estimated residual risk (2012 Report – Volume 2; Public Accounts Committee agreement December 9, 2013

Status – Implemented

SIGA presented its IT risk register to senior management in January 2016. SIGA reported the impact of significant IT risks and responses taken for those risks. In October 2016, SIGA communicated the estimated residual risk to senior management.

3.4 IT Risk Assessment Monitored

We recommended that Saskatchewan Indian Gaming Authority assess the effectiveness of its information technology risk assessment processes and monitor its significant risks on an on-going basis. (2012 Report – Volume 2; Public Accounts Committee agreement December 9, 2013)

Status – Implemented

SIGA assessed the effectiveness of its existing risk assessment process. Based on its assessment, it completed its IT risk assessment policy as described in **Section 3.1**. The policy requires management to annually review its risk assessment processes.

In June 2016, SIGA IT management reviewed its IT risk register. Management reviewed the risks and mitigating strategies to determine if additional or alternative mitigating strategies were required or if there were any additional risks to include in its IT risk register.