Chapter 53
Saskatchewan Indian Gaming Authority Inc.— Information Technology Threat and Risk Assessment Processes

1.0 Main Points

By August 31, 2014, Saskatchewan Indian Gaming Authority Inc. (SIGA) made some progress on two of the four recommendations we made in 2012 related to its information technology (IT) threat and risk assessment processes. However, more work remains.

SIGA needs to complete its IT threat and risk assessment, report to senior management on its risk assessment results, and assess the effectiveness of its IT threat and risk assessment processes.

2.0 Introduction

This chapter reports the results of our follow-up of four recommendations we made in our *2012 Report – Volume 2*, Chapter 35 about 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 original audit. SIGA's management agreed with the criteria in the original 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 recommendations at August 31, 2014, and SIGA's actions up to that date. We found that while SIGA has made some progress on two recommendations, all four recommendations are not fully implemented.

3.1 Complete Plan for IT Threat and Risk Assessment Needed

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 – Partially Implemented

A complete IT threat and risk assessment plan should include timelines, expected participants, scope, and planned steps. Management should review and approve the plan.

SIGA has a draft process map that outlines high-level steps for IT risk identification and assessment. However, the process map does not include all aspects necessary for an IT threat and risk assessment plan. The process map does not include timelines for the identified steps, the expected participants, or the scope of the assessment process. Also, in June 2014, SIGA hired additional IT staff that, as part of their responsibilities, are expected to define formal risk assessment guidelines. At August 31, 2014, guidelines had not yet been developed. SIGA indicated that its internal auditor recently assessed its IT security processes compared to best practice, including threat and risk assessment processes, and provided management with suggestions for improvement. SIGA is currently developing an action plan to address the suggestions.

Without a fully-documented and approved IT threat and risk assessment plan, responsibility for and the timing of the completion of the assessments may be unclear, which may result in delays in the completion of the assessments.

3.2 IT Threat and Risk Assessment Not Yet 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 – Partially Implemented

SIGA has not completed its IT risk assessment. At August 31, 2014, SIGA had documented its analysis of the impact and likelihood for IT risks it faces. However, the analysis does not include planned responses to the identified risks.[1] Senior management has not approved this analysis.

[1] Planned responses to risks should include identification of current controls in place to mitigate risks, planned changes to those controls, the implementation status of any planned changes, and the identification of residual risks that require further action or acceptance.

Without determining the planned responses to identified risks, SIGA does not know if it has satisfactorily addressed its IT risks.

3.3 Reporting on Risk Assessment Results and Assessment of the Effectiveness of Processes Needed

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 – Not Implemented

We recommended that the 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 – Not Implemented

As noted in **Section 3.2**, SIGA's IT risk assessment is not yet complete. As such, it cannot report to senior management on the impact of significant IT risks, responses taken for those risks, and the estimated residual risks.

Without complete information on IT risks, SIGA's senior management is unable to determine if it has developed sufficient responses to IT threats and risks. SIGA indicated that it is currently developing a reporting strategy for senior management.

SIGA has not yet reviewed the effectiveness of its risk assessment processes on an ongoing basis. Ongoing assessment of effectiveness would help SIGA determine if its IT risk assessment and risk responses continue to be appropriate.

SIGA indicated that it plans to review the effectiveness of its information technology threat and risk assessment processes in 2015.