# Chapter 35
# Saskatchewan Indian Gaming Authority Inc.—Information Technology Threat and Risk Assessment Processes

## 1.0 Main Points

The Saskatchewan Indian Gaming Authority Inc. (SIGA) has a significant investment in information technology (IT). SIGA is responsible for ensuring that its IT systems are secure. One aspect of IT security is assessing threats and risks to IT systems and responding appropriately to those threats and risks. We audited SIGA's IT threat and risk assessment processes and found that SIGA needs to:

- Fully document its IT threat and risk assessment plan
- Carry out its documented plan including analyzing the threats and risks, and developing a risk response
- Report the results of the assessment to management
- Review the effectiveness of the assessment process and conduct on-going monitoring

## 2.0 Introduction

SIGA operates Saskatchewan First Nation casinos and ancillary operations.[1] Slot machine profits from SIGA casinos are shared between the First Nations Trust Fund, community develop corporations,[2] and the Provincial Government.

SIGA operates in seven separate locations. In order to operate its casinos and ancillary operations, it has a significant investment in information technology. SIGA uses a variety of purchased and in-house developed software including software for enterprise resource planning, human resources and payroll, help desk system, point of sale, purchasing, scheduling and time card, and security. Although SIGA does not directly operate the slot machine system, it has some software systems related to gaming, including a table games system that tracks the table games revenue and a cash management system that tracks and manages the cash within the SIGA casinos.

We audited SIGA's IT threat and risk assessment processes. SIGA is responsible for ensuring that its IT systems are secure. One aspect of IT security is assessing threats and risks to IT systems and responding appropriately to those threats and risks.

[1] Ancillary operations include food and beverage services, accommodations, gift shops, and live on-stage entertainment.
[2] Community development corporations are non-profit corporations established pursuant to the *2002 Framework Agreement* in communities where SIGA casinos are located. They are to provide grants for economic, social, and cultural development within those communities.

## 3.0 BACKGROUND

A well-defined and carried out IT threat and risk assessment process allows agencies to assess, identify, and modify the overall level of risk to which they are exposed (this is known as their "security posture"). The process includes determining the value of the various types of data generated and stored. This assists agencies in prioritizing and allocating technology resources.[3]

An IT threat and risk assessment should reduce the chance of IT system failure and inefficiencies through improved decision making so that risks may be managed effectively. An effective assessment should help ensure that appropriate levels of controls are implemented to protect information technology assets and related data.

Without adequate IT threat and risk assessment processes, an agency could be exposed to unnecessary risks. This could lead to a failure of the agency to achieve its set objectives, unnecessary expenses to fix a system failure, and/or loss of use of its critical IT systems. Alternatively, an agency may be applying unnecessary controls to mitigate risks that may not be critical to the agency achieving its objectives. This would be an inefficient use of the agency's resources.

We describe good processes for performing IT threat and risk assessments in Section 5.0.

SIGA places significant reliance on IT. If its IT systems fail, operations could be jeopardized and revenue could be lost or additional expenses could be incurred. For example, SIGA's security system relies on the use of IT systems. Inadequate controls over integrity and availability to its security system could result in the system not operating as intended. Without an adequate security system, SIGA could be subject to thefts and frauds, which would result in lower overall net revenue. This loss of revenue would mean there would be less funds available to Saskatchewan's First Nations, charitable and non-profit organizations, and to the General Revenue Fund of the Province.

Failure of IT operations could also result in SIGA not being able to manage and report the results of its operations to its stakeholders on a timely basis. For example, a loss in the use of SIGA's enterprise resource planning systems could result in management not having the appropriate reports to monitor and manage the operations of SIGA. Without the appropriate reports, SIGA may not be able to monitor the results of its table games including monitoring compliance with the approved hold.[4]

## 4.0 AUDIT OBJECTIVE, SCOPE, CRITERIA, AND CONCLUSION

The objective of this audit was to assess whether SIGA had effective IT threat and risk assessment processes for the six-month period ended August 31, 2012.

Saskatchewan Liquor and Gaming Authority (SLGA) owns and manages the slot machine system that SIGA uses. SLGA has contracted with a third party to operate the

[3] Schmittling, p.18.
[4] The hold refers to the expected percentage of the cumulative amount that patrons bet on table games that will be retained by SIGA. The hold is approved by SLGA.

slot machine system. Therefore, the slot machine system is not included in the scope of this audit.

To conduct this audit, we followed the *Standards for Assurance Engagements* published in the *CICA Handbook - Assurance*. To evaluate SIGA's processes, we used criteria based on the work of other auditors and current literature listed in the selected references. SIGA's management agreed with the criteria listed in **Figure 1**.

**Figure 1—Audit Criteria for Adequate IT Threat and Risk Assessment Processes**

To have effective IT threat and risk assessment processes SIGA should:

1. Develop a plan to assess IT threats and risks
2. Carry out its IT threat and risk assessment plan
3. Report to management the results of the assessment
4. Review the effectiveness of the process and plan for on going monitoring of risks

**We concluded that, for the six-month period ended August 31, 2012, SIGA's information technology threat and risk assessment processes were not effective. SIGA needs to:**

- **Fully document its IT threat and risk assessment plan**
- **Carry out its documented plan including analyzing the threats and risks, and developing a risk response**
- **Report the results of the assessment to management**
- **Review the effectiveness of the assessment process and conduct ongoing monitoring**

## 5.0 Good Processes for IT Threat and Risk Assessments

**Figure 2** describes good processes for IT threat and risk assessments applicable for any agency.

**Figure 2—Good Processes for IT Threat and Risk Assessments**

**1. Planning for IT Threat and Risk Assessment**

A good IT threat and risk assessment starts with senior management support. Agencies need senior management support and sufficient resources to plan for and carry out the assessment. This is in terms of both budget dollars and personnel. A well-defined risk management policy[5] would also be an indicator of senior management support of the assessment process. Management should assign someone the responsibility to ensure the assessment is carried out and clearly document the roles and responsibilities of that individual. The individual assigned should have sufficient knowledge and training to carry out the assessments. Agencies would have a documented IT threat and risk assessment plan that would specify:

- Timelines
- Participants
- Scope
- Planned steps

Management would review and approve the documented assessment plan.

[5] A risk management policy would include specifying the requirement for a periodic risk assessment, a risk response plan, reporting to senior management, and on-going monitoring of risks.

**2. Carry Out the IT Threat and Risk Assessment**

There are several key steps in carrying out the IT threat and risk assessment. Agencies need to identify their IT assets and the value of those assets. Value takes into account the business impact of those IT assets. IT assets may include physical equipment, computer programs, personnel, and data. Agencies then need to identify the threats and risks that they face related to those IT assets. Each threat and risk needs to be analyzed as to its impact and the likelihood of the event occurring. For example, an agency may identify a risk that its systems may be unavailable in the event of a power outage at its data centre. If it assesses that a power outage would have a significant impact on its business and there is a high likelihood of it occurring, the agency would need to address this risk. The agency would develop a response to the risks. Possible responses to risks include avoiding the risk, reducing the risk by the addition of further controls, transferring the risk or accepting the risk.[6] The agency would base the response on a cost-benefit analysis to determine the best approach in dealing with each risk. For example, an agency may implement further controls such as installing a backup power supply such as a generator to address the risk of a power outage.

There should be input from key stakeholders across the agency in the assessment process. Without input from all key areas of an agency, the assessment may not adequately address all risks. This can lead to costly and ineffective security measures.[7] Agency-wide input that takes into account the needs of a variety of stakeholders provides for a more effective assessment.

**3. Reporting to Management the Results of the IT Threat and Risk Assessment**

Agencies should provide the completed IT threat and risk assessment to senior management. The report to management should document the significant risks identified and the response taken for each significant risk. The report should also include an estimate or assessment of the residual risk remaining after the agency carries out the initial risk response. Management should approve the residual risk to signify that the agency accepts the remaining risk and does not require the implementation of further controls or risk mitigation steps.

**4. On-going Monitoring and Review of the Effectiveness of the IT Threat and Risk Assessment**

Agencies should periodically monitor their risks to ensure that they have effectively addressed them. Agencies should determine the frequency of the on-going assessment, who would be responsible for on-going monitoring and who should be informed of the results of the monitoring. The on-going monitoring should determine if the assessment of the impact and likelihood of the risk is still appropriate, taking into account the changes to the agency and changes to the environment in which it operates. Also, where an agency implements mitigating controls, the agency should determine if the controls are operating effectively to mitigate the assessed risk as planned. Where there is residual risk that an agency has accepted, the agency should determine if the level of accepted risk is still appropriate for the agency.

Source: See selected references.

# 6.0 Key Findings and Recommendations

In this section, we set out our key findings and recommendations for each criterion.

## 6.1 IT Threat and Risk Assessment Planning

*We expected SIGA to:*

- *Obtain senior management support for the IT threat and risk assessment process including providing adequate budget dollars and personnel*
- *Assign responsibility for threat and risk assessment process*
- *Document its risk management policy*
- *Document in its plan the timelines, expected participants, scope and planned steps*
- *Have the documented plan reviewed and approved by management*

[6] See "risk" in section 7.0.
[7] Bayne, p. 2.

SIGA's senior management supports the IT threat and risk assessment process and has provided funding for a number of consultants' assessments. In 2009, assessments occurred in the area of information security management and impact analysis of SIGA's disaster recovery plan. In 2012, consultants performed a network security assessment and a wireless security assessment. The review of SIGA's information security management was undertaken to develop an information security strategy. This assessment identified a number of IT risks that SIGA faces.

Responsibility for the IT threat and risk assessment process is assigned to a member of senior management. SIGA's IT security policies include a requirement to analyze threats and risks and develop mitigating controls. However, as described in Section 6.2 below, SIGA did not adequately follow those written policies.

Although SIGA had its consultants perform assessments, SIGA did not have a fully documented IT threat and risk assessment plan. SIGA did not set out in its plan the timelines, expected participants, scope and planned steps.

1. **We recommend 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.**

## 6.2 Carry out IT Threat and Risk Assessment Plan

*To carry out its IT threat and risk assessment plan, we expected SIGA to:*

- *Identify IT assets and their value*
- *Identify threats and risks related to the identified assets*
- *Analyze the threats and risks to determine the impact and likelihood*
- *Develop a risk response*
- *Ensure the risk response takes into account an analysis of costs and benefits*

*The assessment should include input from key stakeholders across SIGA.*

SIGA identified its IT assets and their value and has undertaken several initiatives to assess its IT threats and risks. As mentioned above, SIGA contracted with third parties to conduct various reviews of its IT systems and processes. As part of those assessments, the third parties met with a variety of SIGA employees to obtain their perspective of the risks. Through those assessments, a number of risks were identified. For some of these risks, SIGA added further controls to reduce the risks. For example, SIGA is in the process of changing its computer systems so that it can recover from a disaster in a shorter time period.

Although SIGA developed responses to some of its risks, it did not do this for all of them. SIGA did not follow the requirements in its IT security policies as it did not have defined processes to:

- Document its analysis of risks including documenting impact and likelihood in order to determine the significance of each risk
- Document the planned response to address the risks including the costs and benefits of the responses

Without determining the impact and likelihood of the risks occurring and determining the planned response to those risks, SIGA does not know if it has addressed its significant risks.

**2. We recommend 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.**

## 6.3 Report to Management the Results of the Assessment

*We expected SIGA to report to senior management the results of the IT threat and risk assessment including:*

- *Significant risks*
- *Responses taken*
- *Estimated residual risk*

*Management should approve the residual risk.*

SIGA provided management with a report on the results of its IT threat and risk assessments. That report identified the significant risks that could affect its IT systems. However, the report was inadequate because it did not include an analysis of the impact of the risks, the responses SIGA had taken, and the estimated residual risks. Without this information, SIGA's management would be unable to determine if it has developed sufficient responses to the identified risks.

**3. We recommend 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**

## 6.4 Review the Effectiveness of the Assessment Process and Conduct On-going Monitoring

*We expected SIGA to review the effectiveness of its IT threat and risk assessment process and, on an on-going basis, assess:*

- *The impact and likelihood of assessed risks based on changes affecting SIGA*
- *The impact of the mitigating controls to ensure they are still operating effectively*
- *The residual risk to ensure it is still appropriate for SIGA*

*Management should assign responsibility for on-going monitoring and specify the frequency.*

SIGA has not reviewed the effectiveness of its IT threat and risk assessment process. SIGA has not set out how it plans to carry out on-going monitoring of its IT risks. Without on-going monitoring, SIGA is unable to determine if its risk assessment and risk response is still appropriate. For example, when SIGA implemented its enterprise resource planning application, it increased its reliance on its IT systems. SIGA needed to reassess its disaster recovery plan so that it could know that the new application could be recovered in an appropriate time frame in the event of a disaster.

**4. We recommend 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.**

## 7.0 Glossary

**Risk** – the chance of a vulnerability being exploited.[8]

There can be several responses to identified risks, including:

- Risk avoidance (e.g., an agency may avoid risks by relocating its data centre away from a region with significant natural hazards)
- Reducing the risk by the addition of further controls (e.g., an agency may reduce the risk of loss of confidential data through the encryption of all data stored on its computers)
- Transferring the risk (e.g., an agency may transfer a portion of the risk of loss of confidential credit card data through contracting with a reputable third party that specializes in on-line credit card transactions)
- Accepting the risk (e.g., an agency may determine that the costs to implement further controls to protect its computer rooms from destruction through fire outweighs the expected benefit from adding further fire protection equipment)[9]

[8] Communications Security Establishment, p. 281.
[9] Information Systems Audit and Control Foundation, p. 28.

**Residual risk –** the risk that remains after safeguards [controls] have been selected and implemented.

**Threat** – any potential event or act, deliberate or accidental, that could cause injury to employees or assets, and thereby affecting service delivery adversely.[10]

**Vulnerability** – an inadequacy related to security that could permit a threat to cause injury.[11]

## 8.0 Selected References


Bayne, James. An Overview of Threat and Risk Assessment, http://www.sans.org/reading_room/whitepapers/auditing/overview-threat-risk-assessment_76. (24 Sep 2012).

Committee of Sponsoring Organizations of the Treadway Commission, (2012). *Internal Control – Integrated Framework - Draft*, http://www.coso.org/documents/coso_framework_body_v6.pdf. (24 Sep 2012).

Committee of Sponsoring Organizations of the Treadway Commission, (2004). *Enterprise Risk Management – Integrated Framework Executive Summary*, http://www.coso.org/documents/coso_erm_executivesummary.pdf. (24 Sep 2012).

Communications Security Establishment, (2007). *Harmonized Threat and Risk Assessment (TRA) Methodology*, http://www.cse-cst.gc.ca/documents/publications/tra-emr/tra-emr-1-e.pdf. (24 Sep 2012).

Information Systems Audit and Control Foundation, IT Governance Institute. (2009). *The Risk IT Framework*, Rolling Meadows, IL: Author.

National Institute of Standards and Technology, (2002). *Risk Management Guide for Information Technology Systems*, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf. (24 Sep 2012).

Royal Canadian Mounted Police, (1994). *Guide to Threat and Risk Assessment for Information Technology*, Ottawa, Canada: Technical Security Branch, Royal Canadian Mounted Police.

Schmittling, Ron and Munns, Anthony. (2010). Performing a Security Risk Assessment. *ISACA Journal, Volume 1*, 18-24.


[10] Communications Security Establishment, p. 281.
[11] Ibid., p. 282.