Saskatchewan Gaming Corporation

14

Main points

Saskatchewan Gaming Corporation (SGC) needs written procedures for information technology (IT) security to help ensure the confidentiality, integrity, and availability of information systems and data.

SGC also needs a written, tested, and approved disaster recovery plan so it can continue to use IT services in the event of a disaster.

As well, SGC needs to further improve its human resource plan.

For the year ended December 31, 2009, SGC's consolidated financial statements are reliable. SGC had adequate processes to safeguard public resources except as described above, and it complied with authorities governing its activities.

Introduction

Saskatchewan Gaming Corporation (SGC) manages and operates Casino Regina and Casino Moose Jaw under the regulatory authority of the Saskatchewan Liquor and Gaming Authority. *The Saskatchewan Gaming Corporation Act, 1994* established SGC.

Casino Regina is a full-service casino and entertainment centre. Casino Regina has slot machines, table games, a full-service restaurant, and a show lounge. Casino Moose Jaw is also a full-service casino that has slot machines and table games. SGC has a total of 995 slot machines and 42 table games in its casinos.

SGC also owns SGC Holdings Inc. (SGC Holdings). SGC Holdings is a corporation registered under *The Business Corporations Act* (Saskatchewan). SGC Holdings purchases capital assets and leases them to SGC for the operation of the above casinos. SGC's consolidated financial statements include the financial results of SGC Holdings.

SGC's consolidated financial statements for the year ended December 31, 2009 report net revenues of $131.8 million, expenses of $81.1 million, net income of $25.4 million, and assets of $78.4 million.

Audit conclusions and findings

To form our opinions on SGC and SGC Holdings, our Office worked with their appointed auditor, Deloitte & Touche LLP. We used the framework recommended by the *Report of the Task Force on Roles, Responsibilities, and Duties of Auditors*.[1]

In our opinion, for the year ended December 31, 2009:

- **SGC had adequate rules and procedures to safeguard public resources and those of SGC Holdings except for the matters described in this chapter**

- **SGC complied with authorities governing its activities and the activities of SGC Holdings relating to financial reporting,**

[1] To view this report, see our website at www.auditor.sk.ca/rrd.html.

safeguarding public resources, revenue raising, spending, borrowing, and investing

- **the consolidated financial statements for SGC and the financial statements for SGC Holdings are reliable**

Controls to safeguard public resources

Well-performing agencies do three things to help ensure they have effective controls to safeguard public resources. First, they ensure management provides adequate guidance to employees. Second, they require management to establish processes to ensure employees follow the established guidance. Third, they monitor how well they are progressing towards achieving their established goals. We provide our findings in these areas below.

Effective guidance to employees

Agencies should document their policies to provide employees ready guidance to understand and follow the policies. SGC has documented and communicated policies for all areas except those noted below.

Better disaster recovery plan needed

SGC needs a written, tested, and approved disaster recovery plan (DRP) to help ensure that it can continue to use information technology (IT) services in the event of a disaster.

We reported this matter in our 2008 Report – Volume 3. We recommended that SGC prepare a complete disaster recovery plan and assess the need for a business continuity plan. In January 2009, the Standing Committee on Crown and Central Agencies (CCAC) agreed with our recommendation.

SGC places significant reliance on its IT systems to operate. Without an adequate DRP, SGC is at risk of not being able to provide its IT services in a timely manner. Therefore, it may be at risk of not being able to operate its casinos. SGC also needs to assess the requirement for a business continuity plan (BCP) by completing a threat and risk

assessment. A BCP would help SGC recover critical business functions in the event of a disaster.

SGC has a DRP that covers most of its IT systems. This DRP has not been reviewed and approved by management. SGC has an alternate processing site in the event of a disaster and its DRP includes its backup procedures. The DRP should cover all IT systems and include a ranking of SGC's critical applications and documented recovery and restoration steps.

Management told us it has assessed the need for a BCP and concluded that SGC will complete it by 2011.

We continue to recommend that Saskatchewan Gaming Corporation prepare a complete disaster recovery plan.

Better information technology security policies and procedures needed

SGC needs to fully document its IT security procedures and ensure staff follow them. IT security policies and procedures help ensure the confidentiality, integrity, and availability of information systems and data.

We also reported this matter in our 2008 Report – Volume 3. We recommended that SGC fully document its procedures for the security of its information technology systems and ensure that these procedures are being followed. In January 2009, CCAC agreed with our recommendation.

SGC has some IT security policies that define staff roles and responsibilities. The policies identify processes needed for good security including user access, physical security, and virus protection. However, SGC does not have written procedures to monitor compliance with those policies.

SGC must ensure that its staff follow IT policies and procedures. Without adequate monitoring of compliance with IT policies and procedures, SGC's data is at risk of disclosure, modification, or loss.

SGC needs to improve its processes for protecting its network. For example, we found SGC does not always document its monitoring of server log files, firewall logs, security patches, and hardware and software

maintenance. As a result, SGC may not identify attempted or successful security breaches or may have a disruption of service due to inadequate maintenance.

We continue to recommend that Saskatchewan Gaming Corporation fully document its procedures for the security of its information technology systems and ensure that these procedures are being followed.

Management told us that it has completed and approved an IT Security Framework in early 2010. This will aid SGC to develop its procedures for securing its information technology systems.

Better human resource plan needed

SGC needs to improve its human resource plan. Rigorous human resource plans help ensure agencies have the right number of employees, with the right competencies, at the right time.

We have reported this matter since 2007. We recommended that SGC improve its human resource plan by prioritizing its key human resource risks, analyzing human resource gaps, and setting out plans to address human resource gaps. The Standing Committee on Public Accounts considered this matter in 2007 and agreed with our recommendation.

SGC has prepared a human resource plan. The plan includes some discussion about SGC's key human resource risks, but it does not prioritize identified risks (i.e., by considering the likelihood and nature of consequences or risks). SGC has identified general strategies to address its human resource risks. SGC continues to work on detailed action plans to implement the strategies identified.

Also, the human resource plan does not identify SGC's future human resource needs to meet its goals and objectives and it does not identify and analyze anticipated shortfalls or surpluses (gaps).

We continue to recommend that Saskatchewan Gaming Corporation improve its human resource plan by prioritizing its key human resource risks and analyzing human resource gaps.

Glossary

Business Continuity Plan (BCP) – Plan by an organization to respond to unforeseen incidents, accidents, or disasters that could affect the normal operations of the organization's critical operations or functions.

Disaster Recovery Plan (DRP) – Plan by an organization to respond to unforeseen incidents, accidents or disasters that could affect the normal operation of a computerized system. A DRP is only one component of a Business Continuity Plan.

Firewall—Software and/or hardware intended to restrict or block access to a network or computer. Firewalls can be set up to only allow certain types of data through.

Log—A record of computer, network, or application use.

Network—A group of computers that communicate with each other.

Patch—An update to a computer program or system designed to fix a known problem or vulnerability.

Server—A computer that hosts systems or data for use by other computers on a network.

This page left blank intentionally.