Saskatchewan Research Council

24

Main points

In this chapter, we report the results of our audit of the Saskatchewan Research Council (SRC). To carry on its business, SRC relies extensively on its information technology systems. SRC needs to implement appropriate security controls to protect its information technology systems and data from unauthorized access. This includes improving how it manages employee access and how it protects its systems and data from security threats. SRC also needs to know that it can recover systems and data in the event of computer problems or a disaster. SRC should test its information technology disaster recovery plan.

Introduction

The mission of the Saskatchewan Research Council (SRC) is to help the people of Saskatchewan strengthen the economy with quality jobs and a secure environment. It does this through research, development, and transfer of innovative scientific and technological solutions, applications, and services. SRC is a body corporate which receives monies appropriated by the Legislature for these purposes. It is also empowered to conduct research under contract for others and to receive financial assistance pursuant to agreements with other agencies.

In 2007, SRC had revenue of $36.4 million and expenses of $34.1 million. At March 31, 2007, SRC held assets of $26.3 million.

SRC also manages the Saskatchewan Research Council Employees' Pension Plan (Plan). At December 31, 2006, the Plan held assets of $22.4 million and had a surplus of $278,000.

Audit conclusions and findings

In our opinion, for the year ended March 31, 2007:

- **SRC had adequate rules and procedures to safeguard public resources except for the matters reported below**
- **SRC complied with the authorities governing its and the Plan's activities relating to financial reporting, safeguarding public resources, revenue raising, spending, borrowing, and investing**
- **SRC's and the Plan's financial statements are reliable**

Information technology processes need improvement

To carry on its business, SRC relies extensively on its information technology systems.

SRC needs to implement appropriate security controls to protect its information technology systems and data from unauthorized access. This

includes improving how it manages employee access and how it protects its systems and data from security threats.

SRC needs to document who it grants network access to and why. SRC also needs to follow its processes for removing user access. SRC has policies for network passwords. It should ensure that it follows those processes. In addition, SRC should provide guidance to staff on good password practices.

SRC needs to configure its computers and network to protect against security threats. This includes analyzing the risks it faces and implementing controls to reduce the risks to an acceptable level.

1. We recommend Saskatchewan Research Council implement security controls to reduce information technology risks to an acceptable level.

SRC management told us it accepts this recommendation and has developed a plan to address any unacceptable levels of information technology risk.

SRC also needs to know that it can recover systems and data in the event of computer problems or a disaster. SRC has a disaster recovery plan. It should test it.

2. We recommend Saskatchewan Research Council test its information technology disaster recovery plan.

SRC management told us it accepts this recommendation and has developed a plan including timelines to test its information technology disaster recovery plan.