

## Chapter 49

# Saskatoon Regional Health Authority – Protecting IT Infrastructure Follow Up

### 1.0 MAIN POINTS

In 2010, we made six recommendations to help strengthen Saskatoon Regional Health Authority (Saskatoon RHA)'s processes to protect its information technology systems and data. In this chapter, we report that Saskatoon RHA has implemented one of the six recommendations we made in 2010. Saskatoon RHA is now providing reports to the Board of Directors and senior management on the state of its information technology infrastructure. Saskatoon RHA needs to do more work to address our remaining five recommendations. Saskatoon RHA needs to implement adequate information technology policies, effectively restrict access to systems and data, securely configure its computers and network equipment, and monitor the security of its information technology infrastructure. Saskatoon RHA also needs a complete, approved and tested disaster recovery plan.

### 2.0 INTRODUCTION

In 2010, we audited Saskatoon RHA's processes to protect its information technology infrastructure. We reported the results of our audit in Chapter 11D of the 2010 Report - Volume 2 and made six recommendations to help Saskatoon RHA improve its processes.

### 3.0 STATUS OF RECOMMENDATIONS

This section sets out our recommendations and Saskatoon RHA's actions up to August 31, 2012. Saskatoon RHA has implemented one of the six recommendations.

#### 3.1 Implement Adequate IT Policies

We recommended that Saskatoon Regional Health Authority implement adequate information technology policies. (2010 Report – Volume 2; Public Accounts Committee agreement January 19, 2011)

**Status** – We continue to make this recommendation.

Saskatoon RHA requires policies and procedures to effectively manage its information technology infrastructure.

Saskatoon RHA has performed a risk analysis and identified IT policy requirements. It has developed, approved, and implemented some policies that were identified.



However, it has not developed approved policies for reporting IT security incidents, wireless access, and physical security.

### 3.2 Restrict User Access

---

We recommended that Saskatoon Regional Health Authority adequately restrict access to information technology equipment, systems, and data. (2010 Report – Volume 2; Public Accounts Committee agreement January 19, 2011)

**Status** – We continue to make this recommendation.

Saskatoon RHA needs to protect its systems and data by restricting access to authorized users.

Saskatoon RHA has processes to grant and remove user access. However, it does not consistently follow its processes. We found fourteen individuals no longer employed continued to have access to Saskatoon RHA's systems and data.

Continued access of even one employee who no longer works for Saskatoon RHA increases the risk of unauthorized changes to its systems and data.

### 3.3 Configure and Update Computer Equipment

---

We recommended that Saskatoon Regional Health Authority configure and update its computers and network equipment to protect them from security threats. (2010 Report – Volume 2; Public Accounts Committee agreement January 19, 2011)

**Status** – We continue to make this recommendation.

Saskatoon RHA has taken steps to improve its configuration of computer systems and data to protect them from external threats. For example, Saskatoon RHA periodically updates computers and network equipment. However, Saskatoon RHA does not have policies and procedures for updating its computers and network equipment. We found that Saskatoon RHA had not updated some network equipment including security devices (e.g., firewalls).

Failure to update computers and network equipment increases the risk that Saskatoon RHA's data may be inappropriately disclosed, modified, or lost.

### 3.4 Prepare and Test Disaster Recovery Plan

We recommended that Saskatoon Regional Health Authority prepare and test an information technology disaster recovery plan. (2010 Report – Volume 2; Public Accounts Committee agreement January 19, 2011)

**Status** – We continue to make this recommendation.

Saskatoon RHA identified recovery objectives for its top 25 critical applications. Saskatoon RHA also developed a draft disaster recovery plan. The work completed helped Saskatoon RHA to identify existing gaps and recommend steps to manage its risks.

In June 2012, the Board approved a budget of \$1.4 million for backup and recovery solutions. While the work is not yet complete, management expects these steps will help mitigate the current risks while it continues to complete its disaster recovery plan.

### 3.5 Monitor Security

We recommended that Saskatoon Regional Health Authority monitor the security of its information technology infrastructure. (2010 Report – Volume 2; Public Accounts Committee agreement January 19, 2011)

**Status** – We continue to make this recommendation.

Saskatoon RHA has improved its monitoring of systems and data. Reports provided to management include assessments of current risks and known vulnerabilities. Saskatoon RHA hired contractors to help assess the current state of its security. Management has prioritized the weaknesses the contractors identified and has plans to address these issues.

Saskatoon RHA lacks processes for detecting day-to-day security threats. For example, it does not review its logs to identify potential security attacks. This could leave Saskatoon RHA exposed to a security breach.

Saskatoon RHA needs effective monitoring and processes to detect security attacks and potential breaches.



## 3.6 Providing Timely Reports

---

We recommended that Saskatoon Regional Health Authority provide timely reports to the Board of Directors and senior management on the state of its information technology infrastructure. (2010 Report – Volume 2; Public Accounts Committee agreement January 19, 2011)

**Status** – Implemented.

The Board of Directors and senior management received reports describing the current state of risks in Saskatoon RHA's IT infrastructure. Based upon the information, the Board allocated additional funds to address identified risks. Senior management has developed a three year work plan to address the identified risks.

Saskatoon RHA created a committee to develop new IT processes and to monitor the current state of its controls. This committee includes members of senior management and meets regularly. The Audit and Finance Committee of the Board also receives periodic updates on the progress of Saskatoon RHA's three year work plan.