Information technology security

11D

Main points

Saskatoon Regional Health Authority (Saskatoon) did not have adequate processes to protect its information technology (IT) infrastructure. Lack of adequate processes to protect IT infrastructure increases the risk of unauthorized access to Saskatoon's systems and data, unauthorized disclosure of confidential information, and inappropriate changes to data. Also, to provide adequate patient care, Saskatoon must protect its IT infrastructure.

The chapter makes six recommendations to help Saskatoon secure its IT infrastructure. We encourage other regional health authorities to use the criteria described in this chapter to assess the adequacy of their own processes to protect IT infrastructure.

Introduction

The Regional Health Services Act makes Saskatoon Regional Health Authority (Saskatoon) responsible for the planning, organization, delivery, and evaluation of health services in the Saskatoon health region. Saskatoon is responsible to provide health services to over 300,000[1] people at an annual operating cost of over $900 million.[2] It also provides specialized services to the rest of Saskatchewan. Saskatoon employs over 13,000 staff and 847 physicians.[1]

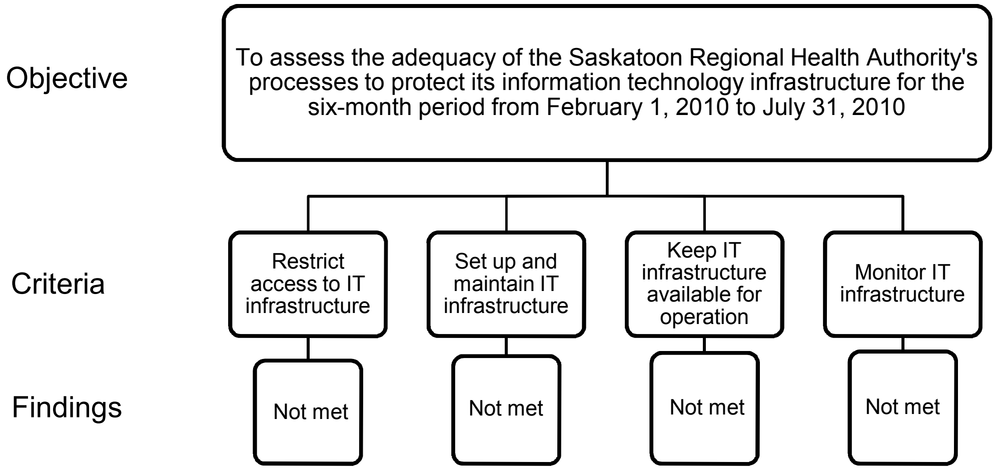
To support the delivery of health care services, Saskatoon uses information technology (IT) systems. For example, Saskatoon uses IT systems for lab results, medical imaging, and patient registration and billing. It needs accurate, appropriate, and timely information from these systems to make wise decisions.[3] Saskatoon also stores confidential patient data in its IT systems. Therefore, maintaining the security of its IT infrastructure is very important to ensure protection of patient data.

Over the next few years, Saskatoon expects to increase its use of IT systems through the Government's implementation of electronic health record systems. These systems will enable easier access to complete patient data by health care providers. They will also require increased security controls to ensure accuracy, completeness, and confidentiality of the patient data.

To provide adequate patient care, Saskatoon must protect its IT systems and data. Saskatoon's IT systems and data reside on its network and computer equipment. Saskatoon needs to protect its equipment from loss, damage, and unauthorized changes. Failure to do so could result in disclosure of patient data, incorrect information, and inadequate patient care.

[1] *Saskatoon Regional Health Authority, 2009-2010 Annual Report*, p. 5.
[2] Ibid, p. 91.
[3] *Saskatoon Regional Health Authority, 2008-2009 Annual Report*, p. 42.

Objective and criteria



Objective

To assess the adequacy of the Saskatoon Regional Health Authority's processes to protect its information technology infrastructure for the six-month period from February 1, 2010 to July 31, 2010

Criteria

Restrict access to IT infrastructure

Set up and maintain IT infrastructure

Keep IT infrastructure available for operation

Monitor IT infrastructure

Findings

Not met

Not met

Not met

Not met

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

Conclusion and recommendations

The Saskatoon Regional Health Authority did not have adequate processes to protect its information technology infrastructure for the six-month period from February 1, 2010 to July 31, 2010.

Inadequate processes to protect IT infrastructure increase the risk of unauthorized access to Saskatoon's system and data, unauthorized disclosure of confidential information, and inappropriate changes to data. The following recommendations are designed to help Saskatoon strengthen its controls to protect its systems and data.

1. We recommend that Saskatoon Regional Health Authority implement adequate information technology policies.

2. We recommend that Saskatoon Regional Health Authority adequately restrict access to information technology equipment, systems, and data.

3. **We recommend that Saskatoon Regional Health Authority configure and update its computers and network equipment to protect them from security threats.**

4. **We recommend that Saskatoon Regional Health Authority prepare and test an information technology disaster recovery plan.**

5. **We recommend that Saskatoon Regional Health Authority monitor the security of its information technology infrastructure.**

6. **We recommend that Saskatoon Regional Health Authority provide timely reports to the Board of Directors and senior management on the state of its information technology infrastructure.**

Detailed findings by criterion

In the following sections, we describe our expectations (in italics) and findings for each criterion.

Restrict access to IT infrastructure

We expected Saskatoon to have adequate physical access and user access processes to protect the IT infrastructure from unauthorized access.

Good physical control means protecting IT infrastructure from harm. Physical access controls protect all computers and network devices from unauthorized access. For example, security controls should physically prevent unauthorized users from entering a data centre.

User access controls limit use of an IT system to only approved people or processes. A common example of a user access control is a username and a password. The username identifies the user and the password grants access.

Protecting systems from unauthorized access is more critical with the increased use of the internet, automated processes, and multiple locations.

Saskatoon did not have adequate documented policies and procedures for physical protection of its IT equipment. It used locked rooms (e.g., server rooms) to protect most of its computer equipment in Saskatoon. However, at some of its facilities located in rural Saskatchewan, network equipment was located in areas open to the public.

Saskatoon has documented user access policies and procedures for granting and removing user access and for password requirements. However, Saskatoon did not consistently follow its policies during the audit period. For example, some staff no longer employed by Saskatoon continued to have access to systems and data. In addition, some accounts used to access the network did not have passwords set to expire.

Inadequate processes to restrict access to IT infrastructure increases the risk of damage, loss, or inappropriate use of systems and data.

Set up and maintain IT infrastructure

We expected Saskatoon to have processes to adequately set up (i.e., configure) and update its IT infrastructure against security threats. Adequate processes require approving and testing system changes before implementation.

Saskatoon did not have adequate documented policies and procedures for the configuration of its computers and network equipment. Some of its equipment did not appropriately restrict access. Processes for remotely accessing systems and data were inadequate. In one case, a wireless network used inadequate encryption. The weak encryption could allow an unauthorized user to see data sent on the wireless network. Without appropriate security, unauthorized individuals could obtain access to systems and data without physically being present in restricted areas.

Saskatoon did not have adequate documented policies and procedures for updating (i.e., patching) its IT equipment. Saskatoon did not update its IT equipment on a timely basis. In some cases, it did not update computers and network equipment for over a year. Improperly maintained equipment may not work as required.

Keep IT infrastructure available for operation

We expected Saskatoon to have adequate processes to ensure its systems and data are available for operation when needed.

Even with good backup and recovery procedures, Saskatoon may not be able to continue its operations if a major problem occurs. Therefore, it should have a contingency plan to recover operations in the event of a disaster like a fire or flood. This includes building capacity, when cost effective, into systems so a disaster in one location will not cause applications to quit running at other locations where employees are still able to work.

Saskatoon has established processes to backup its data. It has also identified its critical systems and has defined some recovery time requirements. However, it did not have a complete disaster recovery plan (DRP). Management told us it plans to develop and implement detailed recovery plans for all critical systems, including downtime procedures that staff should follow if a system is unavailable. When complete, Saskatoon should test its DRP regularly to ensure the plan will work as required.

Without an adequate DRP, systems and data may not be available when needed.

Monitor IT infrastructure

We expected Saskatoon to monitor compliance with security policies and procedures. This includes monitoring contractors who perform work on its behalf. We also expected Saskatoon to have processes to identify and resolve security threats.

Saskatoon did not have adequate IT security policies and procedures. Management told us it plans to draft policies and procedures based on its threat and risk assessment.

Saskatoon did not have documented policies and procedures for monitoring or responding to IT security threats. For example, it did not monitor potential security alerts. Nor did it have processes capable of detecting inappropriate activity on its network. Without adequate monitoring of its systems, Saskatoon would not be aware of unauthorized attempts to access IT systems and data or successful security breaches. Management told us that it plans to hire an IT security officer in late 2010 whose responsibilities will include implementing a process to monitor IT security compliance.

Saskatoon has a committee to oversee IT strategy and infrastructure. The committee includes members from senior management. However, the committee did not meet regularly during the audit period. Without regular meetings, the committee may not be able to assess and report upon the adequacy of the Saskatoon's IT infrastructure including services provided by external service providers.

Senior management and the Board of Directors need to monitor the adequacy of the Saskatoon's IT infrastructure by reviewing periodic reports from the committee.

Selected references

Canadian Institute of Chartered Accountants (CICA). (2003). *Trust services principles and criteria*. Toronto: Author.

International Organization for Standardization. (2005). ISO/IEC 27002:2005(E). *Information technology – Code of practice for information security management; 2nd Edition*. Geneva: Author.

IT Governance Institute. (2006). IT Control Objectives for Sarbanes-Oxley: *The role of IT in the design and implementation of internal control over financial reporting, 2nd Edition*. Rolling Meadows, IL: Author.

The Information Systems Audit and Control Foundation. (2005). *CoBiT4.0*. Rolling Meadows, IL: Author.

Glossary

Account—A unique identity set up on a computer or network that allows access to specific systems and data.

Application—A software program. This includes programs such as word processors, spreadsheets, database programs, accounting programs, etc.

Backup (noun)—A copy of systems or data to be used when the originals are not available (e.g., because of loss or damage).

Configure—To set up or arrange in order to achieve a specific purpose (e.g., maximize security).

Data centre—A central location for computer network hardware and software, especially storage devices for data.

Disaster recovery plan—A plan for an organization to restore necessary IT services in the event of an emergency or disaster. A disaster recovery plan is one part of a larger, organization-wide business continuity plan.

Electronic health record—A person's health record designed to be accessed online from many separate, compatible systems within a network.

Encryption—A method of putting information in code so that only authorized users will be able to see or use the information.

IT infrastructure—An organization’s computer and network equipment.

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.

Physical access controls—The controls in place at an organization that restrict unauthorized people from gaining physical access to computers or network equipment. Examples include locked doors and cabinets, and video surveillance systems.

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

User access controls—The controls in place at an organization to restrict use of systems or data to those who have been authorized. These include physical controls such as locked doors or cabinets, as well as computer and network controls such as establishing accounts with specific access rights, requiring passwords, etc.