IT security

11F

This page left blank intentionally.

Providing information technology services to clients

The Health Information Solutions Centre (HISC) is a branch of the Department of Health. The Department uses HISC to develop and integrate health care information systems, support the use of information for health care planning and accountability, and manage the provincial network that links the Department and health regions, facilities, and agencies.[1]

HISC's clients include government agencies such as the regional health authorities, the Saskatchewan Association of Health Organizations, Saskatchewan Cancer Agency, as well as other health-related agencies in the province. According to the Department, at March 31, 2007, HISC hosted 35 systems for health regions and agencies, for example:

- Pharmacy Information System (PIP)
  - accessed by health care professionals to assist in identifying potential drug interactions and other prescription management activities
- Saskatchewan Immunization Management System (SIMS)
  - helps public health nurses across Saskatchewan provide immunization services to children
- Chronic Disease Management (CDM) System
  - used by participating primary care physicians to better manage the care of chronic disease patients
- Shared Client Index (SCI)
  - provides identification services for all patients who received care in a Saskatchewan hospital
- Saskatchewan Surgical Care Network (SSCN)
  - used to track surgical waiting times and provide the information necessary to allocate surgical resources and reduce patient wait times
- Integrated Clinical Systems
  - support the delivery of front-line services in hospital admitting, health records, pharmacy and laboratory departments as well as home care programs[2]

HISC has also begun to implement an electronic health record system intended to help health care providers share information (including

[1] http://www.health.gov.sk.ca/about/ (05 Oct. 2007).
[2] http://www.health.gov.sk.ca/data-centre (05 Oct. 2007).

pharmacy, digital imaging, and lab results) anywhere in Saskatchewan where residents seek treatment.[3]

To effectively support Department and client systems and their use, HISC needs adequate controls to protect its data centre and network. Unauthorized disclosure, loss, or inappropriate modification of information could harm individuals and larger population groups. Inaccurate or missing information would impede effective planning and decision making at the regional and provincial level. Inadequate controls to protect the availability of systems or information could interfere with providing much needed health services.

Audit objective and criteria

The objective of our audit was to assess whether the Health Information Solutions Centre of the Department of Health had adequate controls to protect the confidentiality, integrity, and availability of client information technology systems and data for the period March 1, 2007 to August 31, 2007.

We used criteria to assess the Department's processes. The criteria are based on the *Trust Services Criteria and Principles* authored by The Canadian Institute of Chartered Accountants and international standards, literature, and reports of other legislative auditors. The Department agreed with the criteria.

The criteria, set out in the exhibit below, describe the key processes that we expected the Department to use to secure client systems and data.

[3] Department of Health Annual Report 2006-07, p.3.

Exhibit—Audit Criteria

To ensure the Department has adequate controls to protect the confidentiality, integrity, and availability of client information technology systems and data, it should:

1. **Show management commitment to security**

   1.1 Responsibility for security is clearly defined
   1.2 A threat and risk assessment has been performed
   1.3 Information technology planning supports security
   1.4 Management has approved security policies and procedures
   1.5 Management monitors security
   1.6 There are information technology service delivery contracts with clients

2. **Protect client systems and data from unauthorized access**

   2.1 User access controls protect the client systems from unauthorized access
   2.1 Physical security controls protect the data centre from unauthorized access

3. **Ensure client systems and data centre are available for operation**

   3.1 System and data backups occur and are tested
   3.2 Disaster recovery and business continuity plans are in place

4. **Ensure the integrity of client systems and data**

   4.1 Change management processes exist and are followed
   4.2 Computer operation processes exist and are followed

Throughout our audit, we followed *The Standards for Assurance Engagements* established by The Canadian Institute of Chartered Accountants.

While this audit focused on the Department's controls at the Health Information Solutions Centre, the confidentiality, integrity, and availability of client systems and data also require strong security controls at clients. For example, clients need good physical security processes to ensure only authorized users have access to their systems and data. Client security controls were not included in the scope of this audit. Both HISC and its clients must have strong security processes to avoid placing systems and data at risk. In Chapter 11C, we report on regional health authorities, which are clients of HISC.

Audit conclusion

Based on our examination at the Department against the above criteria, we reached the following conclusion.

The Health Information Solutions Centre of the Department of Health did not have adequate controls to protect the confidentiality, integrity, and availability of client information technology systems and data for the period March 1, 2007 to August 31, 2007.

We describe our key findings in the following section.

Key findings by criterion

Show management commitment to security

Commitment includes setting up a strong organizational structure that clearly defines who is responsible for security. A strong information technology (IT) division is led by a member of senior management. It has a steering committee to ensure the IT division meets client needs. Commitment also includes implementing and monitoring compliance with security policies and procedures.

We note that HISC was undergoing significant organizational change during the period of our audit. This included the amalgamation of its main data centres and the reorganization of its information technology staff. The amended organizational structure clearly defines who is responsible for security.

HISC is led by a member of senior management. Management has a clear understanding of its security responsibilities. HISC has a committee for discussing IT issues with its clients.

HISC is in the process of updating and consolidating its security policies and procedures. It has drafted a security policy, based on international standards, to replace outdated policies. HISC has to implement its draft security policies and procedures. HISC also needs to share the policies and procedures throughout the branch so that staff are aware of their security responsibilities.

HISC management needs to improve how it monitors security. HISC set up a quality assurance group to help evaluate security controls. The quality assurance group should evaluate network security controls. Management could also monitor security by receiving regular security reports from staff or from independent reviews. Without effective monitoring processes, HISC may not identify weaknesses that could result in a security breach.

HISC uses service level agreements to manage client expectations. These agreements clearly set out the responsibilities of HISC and its clients. However, HISC is not meeting its service level commitments related to disaster recovery and protecting systems from security threats (firewall management).

1. **We recommend the Health Information Solutions Centre of the Department of Health approve and implement its draft security policies and procedures.**

2. **We recommend the Health Information Solutions Centre of the Department of Health monitor the security of systems and data by reviewing regular reports on the adequacy of its controls.**

3. **We recommend the Health Information Solutions Centre of the Department of Health meet its service level commitments to its clients related to firewall management and disaster recovery.**

Protect client systems and data from unauthorized access

We expect HISC to have adequate physical access and user access processes that protect the clients' systems and data from unauthorized access.

Good physical controls means protecting IT infrastructure from harm. Physical access controls protect all computers, network devices, disk drives, backup devices, and wiring from unauthorized access. For example, HISC should physically prevent unauthorized users from entering its data centre.

User access controls ensure only approved people or processes can use an IT system. 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 clients using one data centre. HISC should protect the data centre by configuring, updating, and monitoring its systems against security threats.

HISC has good physical security controls for protecting its IT infrastructure. HISC secures its data centre with several layers of physical security that are designed to prevent unauthorized access. HISC has also implemented video surveillance processes for high security areas.

HISC has processes for granting and removing user access. HISC should follow its processes by ensuring only authorized users have access to systems and data. Inappropriate user access could result in disclosure, loss, or modification of the information hosted by HISC.

HISC should follow its defined password standards. For example, we identified over 200 accounts that were not set to expire. The passwords on these accounts are not changed on a timely basis and did not meet HISC's password standard. HISC also needs to make sure that administrator passwords follow standards and are appropriately secured.

4. We recommend the Health Information Solutions Centre of the Department of Health follow its procedures for controlling user access to systems and data.

HISC has established a network architecture that could provide an appropriate foundation for secure service delivery. To provide secure service delivery, HISC needs to make sure computers and network equipment (e.g., firewalls, routers, and switches) are properly configured (i.e., set to operate appropriately), updated against known security threats, and effectively monitored.

HISC manages over 150 servers, 400 firewalls, and other computer equipment. HISC has not documented standard configurations for its computers and network equipment. Nor has it configured computers and network equipment appropriately. We found weaknesses with computers and network equipment that could result in unauthorized access to systems and data.

HISC should regularly update its computers and network equipment against known security risks. HISC has installed some security updates on computers. However, HISC does not follow adequate processes to identify needed updates and make timely changes. As a result, key computer updates have been missed and key network equipment has not been updated to address known security risks.

HISC also needs to effectively monitor all key computers and network equipment. HISC does monitor a network security device that is used to protect its data centre. However, HISC is not reviewing logs of other key equipment used to protect systems and data from security threats. Without adequate review of log information, HISC may not be able to detect network attacks or security breaches.

5. We recommend the Health Information Solutions Centre of the Department of Health protect systems and data from security threats by adequately configuring, updating, and monitoring its computers and network equipment.

Management told us that it plans to purchase additional equipment for updating and monitoring its systems and data. Management expects to have the equipment by March 31, 2008.

Ensure client systems and data are available for operation

We expect HISC to have strong processes to ensure client systems and data are available for operation when needed.

Even with good backup and recovery procedures, an agency may not be able to continue its operations if a major problem occurred. Therefore, agencies should have strong contingency plans 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.

HISC needs to improve its processes for backing up systems and data. This includes having documented system and data backup procedures.

HISC has agreed to have a disaster recovery plan for the data centre and client systems. The agreements require that HISC maintain and annually test the disaster recovery plan. The disaster recovery plan is not completed, is outdated, and has not been regularly tested. HISC needs an approved and tested disaster recovery plan for its data centre and client systems.

HISC has been able to restore individual systems and data when required (for example, when files need to be restored or computers replaced). However, without an approved and tested plan, HISC does not know if it could restore systems and data in the event of a disaster. This could result in systems, data, and services being unavailable when needed.

6. **We recommend the Health Information Solutions Centre of the Department of Health have an approved and tested disaster recovery plan for systems and data.**

Management told us that it has purchased additional equipment for data backup and plan to install it by March 31, 2008. Management has also begun to develop a revised disaster recovery plan for its data centre.

Ensure the integrity of the client systems and data

We expect HISC to have processes for maintaining the integrity of client systems and data by implementing strong change management and IT operation processes. The processes should ensure system changes are approved and tested before implementation. HISC also needs to ensure that it has strong processes for running and maintaining its data centre.

HISC has processes for making changes to systems and data. HISC needs to follow these processes by updating its systems against known security risks. HISC also needs to have strong processes for maintaining and monitoring systems and data. These findings are described earlier under the heading "Protect client systems and data from unauthorized access."

Selected references

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

Canadian Institute of Chartered Accountants. (CICA). (1998). Information technology control guidelines. Toronto: Author.

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

International Organization for Standardization. (2005). ISO/IEC 17799:2005(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.

This page left blank intentionally.