Chapter 7
Central Services—Information Technology Division—Data Centre

1.0 Main Points

The Information Technology Division of Central Services (formerly called and described in this chapter as the Information Technology Office or ITO) delivers information technology (IT) services to 26 ministries and agencies (clients). Even though ITO uses a third-party service provider to provide data centre services, it remains responsible for security of the data centre.

While ITO made some improvements to its security processes during April to December 2013, ITO has not fully addressed the recommendations we made in prior years. ITO needs to:

- Follow its risk management processes to help ensure risks to the data centre are appropriately managed
- Obtain complete and timely information to determine whether the service provider is meeting ITO's security requirements
- Adequately restrict user access to all IT equipment and systems
- Fully secure all key servers and network equipment
- Have an approved and tested plan to recover systems and data in the event of a disaster
- Adequately inform its clients whether ITO is effectively securing their systems and data, including consequences of any issues
- Complete security policies that set a minimum IT security standard for clients to follow

As a result, there is continued risk that systems and data will not be available when required, of inappropriate modification of systems or data, and of unauthorized access. For example, in 2013, ITO provided an individual employed by another government agency with inappropriate access to the data centre. This individual gained unauthorized access to servers that housed client data. While ITO removed this access after its third-party service provider's security processes detected the unauthorized access, the intrusion highlights the need for ITO to take prompt action to resolve the above-noted security weaknesses.

2.0 Introduction

Since May 2012, ITO has delivered IT services to its clients (see **Section 7.0** for ITO's client list at December 2013). ITO indicates that it delivers IT services covering 45,000

electronic assets (e.g., computers, printers) and 1,500 applications. Over 12,000 staff of its clients located throughout the province use these electronic assets and applications.

Under agreements with each of its clients, ITO is responsible for providing secure IT services. As explained in **Section 3.0**, ITO provides some IT services directly and since December 2010, it has outsourced the data centre to a third-party service provider.[1] ITO remains responsible for meeting the requirements it has agreed upon with clients.

This chapter reports the results of our 2013 audit of whether ITO had effective processes to secure the data centre. We perform this audit annually to support our audits of ITO's clients.

3.0 ITO Services

3.1 ITO Services Provided Directly by ITO

ITO is responsible for providing IT services directly to clients, including:

- Managing the relationship between ITO and its clients
- Maintaining a help desk to respond to client requests (e.g., granting/removing access to systems/data, password resets) and to help resolve problems encountered by client staff
- Monitoring and following up on security threats identified by security tools (e.g., firewalls)
- Reviewing and following up on security information provided by ITO's service provider
- Providing computers to client staff
- Providing application development and change management

3.2 ITO Services Provided through its Service Provider

Since December 2010, ITO has engaged a third-party service provider to deliver data centre services to ITO clients on ITO's behalf. ITO's agreement with the service provider sets out the roles and responsibilities of both ITO and the service provider.

The service provider is responsible for operating the data centre. The data centre includes all servers that operate the network and host applications. The data centre also includes network and telecommunications equipment that allow computers to send/receive data, systems used to backup data, and mass storage devices used to store client systems and data. The service provider is also responsible for implementing strong physical security controls to prevent unauthorized access.

[1] ITO directly operated a data centre from 2005 until December 2010.

ITO and its service provider have agreed on how the data centre and all related equipment are to be configured, managed, and maintained. ITO and its service provider revisit these requirements on a periodic basis.

ITO requires the service provider to annually report on its compliance with agreed-upon requirements. Any equipment not in compliance with the agreed-upon requirements must either be remedied by the service provider or exempted by ITO/clients. For example, ITO/clients may exempt a server from receiving security updates if there is a risk that applications on that server may not run properly with the latest server updates.

4.0 Importance of Effective Security Processes

Information technology allows people to access systems and data from anywhere in the world at any time. This opportunity creates a corresponding challenge—how to effectively secure systems and data against cyberattacks.[2] Organizations need effective security processes to protect the confidentiality, integrity, and availability of systems and data against cyber threats.

Public Safety Canada has reported that the frequency and severity of cyberattacks is accelerating.[3] Saskatchewan is not immune to this threat; nor can governments ever fully protect themselves against all cyberattacks. Human error or intentional malicious acts will always make systems and data susceptible to attacks. However, well-secured systems are better able to defend against attacks, detect potential failures, and limit loss if systems and data are breached. For those reasons, effective security processes are of vital importance.

To protect the security of systems and data against cyberattacks, ITO needs to ensure that its service provider implements effective security processes and that ITO's clients adhere to effective security requirements. This is because a weakness involving the service provider or at a client location could pose risks to ITO and all its clients. Without security controls, someone could gain unauthorized access, obtain confidential information, inappropriately modify systems or data, or perform acts that could affect availability.

5.0 Audit Objective, Scope, Criteria, and Conclusion

The objective of our audit was to assess whether the Information Technology Division of the Ministry of Central Services had effective processes to secure the data centre for the nine-month period of April 1, 2013 to December 31, 2013.

The audit did not assess the effectiveness of security controls (e.g., user access controls) for specific client systems (e.g., financial accounting or payroll systems). We assess security controls in our audits of ITO's clients.

[2] Cyberattacks include the unintentional or unauthorized access, use, manipulation or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information. www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf, p. 3 (31 March 2013).
[3] Ibid.

We examined both ITO's and its service provider's controls and processes used to secure the data centre, including network device configuration, server patch levels, and physical security at the data centre. We also examined ITO's agreements, minutes, reports, and policies.

To conduct our audit, we followed the standards for assurance engagements published in the *CPA Canada Handbook – Assurance*. To evaluate ITO's processes, we used criteria (see **Figure 1**) based on the work of other auditors and literature listed in the selected references. The criteria are primarily based on the *Trust Services Principles, Criteria, and Illustrations* authored by the Canadian Institute of Chartered Accountants (CICA) and the American Institute of Certified Public Accountants. ITO management agreed with the criteria.

Figure 1—Audit Criteria

To have effective processes to secure the data centre, the Information Technology Office of the Ministry of Central Services should:

1. **Demonstrate management commitment to security**
   - 1.1 Have an adequate agreement with its service provider
   - 1.2 Effective threat and risk assessments are performed
   - 1.3 Management approves effective security policies and procedures
   - 1.4 Management effectively monitors security including its service provider
2. **Protect systems and data from unauthorized access**
   - 2.1 Effective user access controls protect systems from unauthorized access
   - 2.2 Effective physical security controls protect the data centre from unauthorized access
3. **Ensure systems and data centre remain available for operation**
   - 3.1 Effective backup processes exist and are followed
   - 3.2 Effective disaster recovery plans exist and are tested
4. **Ensure the integrity of systems and data**
   - 4.1 Effective change management processes exist and are followed
   - 4.2 Effective operational processes exist and are followed

We concluded that for the period of April 1, 2013 to December 31, 2013, the Information Technology Division of the Ministry of Central Services had effective controls to secure the data centre except that it needs to:

- **Follow its risk management processes to help ensure risks are appropriately managed**
- **Obtain complete and timely information to determine whether the service provider is meeting the Information Technology Division's security requirements**
- **Adequately restrict user access to all IT equipment and systems**
- **Fully secure all key servers and network equipment**
- **Have an approved and tested plan to recover systems and data in the event of a disaster**
- **Adequately inform clients whether the Information Technology Division is effectively securing their systems and data, including consequences of any issues**
- **Complete security policies that set a minimum IT security standard for clients to follow**

6.0 Key Findings And Recommendations

In this section, we set out our key findings and recommendations.

6.1 Need to Effectively Follow Threat and Risk Assessment Processes

Although ITO has designed processes to document, assess, and respond to key risks, it did not consistently follow them during the audit period.

ITO has documented policies and procedures for risk management that specify who needs to do what, when, and how often. For example, the policies and procedures specify that a risk register that identifies, describes, categorizes, and assesses key risks is to be maintained. The policies and procedures require that a risk officer meet with the executive committee on a quarterly basis to provide an update on progress made to address key risks.

However, ITO has not complied with the requirements of its risk management processes. For example, it has not updated the risk register to reflect significant changes to its senior management team during the audit period. As a result, we found that the majority of risk owners identified in the register were either no longer in those roles or no longer employed by ITO. Also, the risk register did not clearly define who was the risk officer. While management advised us that the ITO executive committee reviewed key risks in April 2013, quarterly reviews, as required by ITO policy, did not occur during the audit period.

Non-compliance with established risk management policies and procedures increases the likelihood of unauthorized access and loss.

1. **We recommend that the Information Technology Division of the Ministry of Central Services follow its established processes to identify and manage risks related to the data centre.**

6.2 Need to Effectively Monitor Whether the Service Provider Meets ITO Security Requirements

We recommended that the Information Technology Division of the Ministry of Central Services monitor whether its service provider meets its security requirements. (2011 Report – Volume 2; Public Accounts Committee agreement June 25, 2012)

Status – Partially Implemented

ITO's processes for monitoring its service provider did not significantly change from our previous audit.

ITO continued to have agreements with the service provider that outline security requirements for configuring and maintaining server and network equipment. ITO management also met regularly with its service provider and received periodic reports from the service provider on servers that use unsupported software.

Under its agreements with the service provider, ITO is to receive annual security reports called compliance scan reports. These reports are to document the service provider's compliance with defined security requirements for the data centre network and for servers.

In our previous audit, we reported that ITO received compliance scan reports for network equipment but not servers. In December 2013, ITO received compliance scan reports for servers and network equipment from the service provider. However, the scope and frequency of compliance scan reports received provide limited assurance on the adequacy of security controls implemented by the service provider at the data centre. For example, the network compliance scan reports did not show whether administration access granted to some network equipment was appropriate, the status of updates to network equipment or whether there were vulnerabilities that could expose network equipment.

ITO needs timely and complete information to monitor its service provider. ITO could require further reporting from its service provider, perform direct verification work itself, or have vulnerability assessments performed by third parties to assess security. Without timely and complete information on data centre vulnerabilities, there is increased risk that ITO will not be able to take timely corrective action to resolve weaknesses. As described in **Section 6.4**, we found weaknesses with configuration and patch management which means that server and network equipment were not properly secured.

6.3 Need to Adequately Restrict Access

We recommended that the Information Technology Division of the Ministry of Central Services adequately restrict access to systems and data. (2012 Report – Volume 2; Public Accounts Committee has not yet considered this recommendation)

Status – Partially Implemented

While ITO requires user identification accounts and passwords to access all systems and data, and most systems follow ITO policy requirements for user identification and passwords, some do not.

At December 2013, ITO had exempted some user accounts from following its established standards. For example, it allowed some passwords for accounts to not expire. Weak password controls increase the possibility that a password may be compromised and used to gain unauthorized system access.

Also, ITO processes for remotely accessing some network equipment and systems and data need strengthening. For example, ITO has older remote access methods that are still accessible and need better security. Not having appropriate security for remote access increases the risk that individuals may obtain unauthorized access to systems and data without being physically present.

6.4 Need to Adequately Configure and Update Servers and Network Equipment

We recommended that the Information Technology Division of the Ministry of Central Services adequately configure and update its server and network equipment to protect them from security threats. (2012 Report – Volume 2; Public Accounts Committee has not yet considered this recommendation)

Status – Partially Implemented

ITO's processes for configuring and updating server and network equipment did not significantly change from our previous audit.

Although ITO's service provider patched most servers on at least a quarterly basis, patching on all servers was not complete for all known vulnerabilities. Also, some servers were using unsupported software. Use of unsupported software means no security updates were available for these servers. This increases the risk of unauthorized access to systems and data.

ITO did not improve its firewall configurations during the audit period. As noted in our past reports, ITO uses firewalls to protect its data centre. While data centre firewalls were at appropriate locations and were monitored, they were not properly configured. ITO's firewall rules did not effectively restrict access to the data centre because ITO did not effectively define the firewall rules that its service provider must follow. Inadequate firewall rules increase the risk of a security breach.

In prior years, we reported that without adequate configuration, someone could gain unauthorized access, obtain confidential information, inappropriately modify systems or data, or perform malicious acts that could affect availability. During the audit period, an individual employed by a government agency gained inappropriate and unauthorized access to the data centre network and some client servers. The service provider's security processes detected the intrusion. However, this intrusion highlights the need for ITO to take prompt action to resolve its security configuration weaknesses.

Management noted that it addressed the specific issues that allowed the individual to obtain unauthorized access and reassessed its controls to protect the data centre from future unauthorized access. Senior management subsequently received and approved a multi-year plan to resolve identified configuration weaknesses, starting with a current gap analysis and an assessment of the firewall rules.

6.5 Complete and Tested Disaster Recovery Plan Required

We recommended that the Information Technology Division of the Ministry of Central Services have a disaster recovery plan for the data centre and client systems. (2006 Report – Volume 3; Public Accounts Committee agreement April 3, 2007)

Status – Not Implemented

ITO continued to not have a complete and tested disaster recovery plan for the data centre and for some mission-critical client systems and data.

ITO experienced significant change to its senior management team during the audit period. No staff members took ownership for updating key documentation prepared in prior years. As a result, documentation was not complete as staff responsibilities for disaster recovery and ongoing business continuity processes were not clearly documented or defined. Unless staff know who is to do what in the event of a disaster, there will not be an effective response.

ITO has identified the need to improve its disaster recovery planning and testing processes. According to the ITO, depending on availability of funding, it would like to set up a data centre contingency site to provide critical IT services to ITO and its clients in the event the primary data centre is unavailable for use.

At December 31, 2013, ITO's agreement with its service provider only requires the service provider to make "best efforts" in the event of a disaster. If a disaster occurred, it is not clear if the best efforts recovery would meet client needs, how long it would take for systems and data to be fully operational, or at what cost. As a result, neither ITO nor its clients know whether critical IT systems and data could be restored when needed in the event of a disaster and will not know until testing is performed, or an actual disaster occurs. These conditions could result in critical IT systems, data, and services not being available to the Government and the people of Saskatchewan when needed (e.g., correctional information system, student loan system, etc.).

6.6 Need to Provide Relevant and Timely Security Reports to Clients

We recommended that the Information Technology Division of the Ministry of Central Services provide relevant and timely security reports to its clients. (2009 Report – Volume 3; Public Accounts Committee agreement June 18, 2010)

Status – Partially Implemented

Like ITO itself, its clients need information from ITO to enable them to monitor the effectiveness of ITO's security services. ITO's clients need to know that ITO—their service provider—is doing its job. They need timely and relevant security reports to allow effective monitoring. They need to know about any security issues that exist and how these issues impact their systems and data.

ITO did not significantly improve its reporting processes to clients to enable clients to monitor whether their systems and data were secure. Also, we did not find evidence that ITO reported effectively to clients regarding the intrusion we described earlier in this chapter. Management advised that it informed senior management at affected agencies about the security intrusion.

6.7 Complete Client Security Policies Required

We recommended that the Information Technology Division of the Ministry of Central Services establish information technology security policies for its clients.
(2008 Report – Volume 3; Public Accounts Committee agreement December 10, 2008)

Status – Partially Implemented

ITO developed additional security policies and procedures for clients during the audit period. For example, ITO drafted a new acceptable use policy that would apply to all client staff. However, this work is not complete. ITO has draft policies in a number of areas (e.g., physical security, access control, incident management). ITO is working with clients to review, approve, and implement new policies and procedures.

7.0 ITO Client List at December 2013

Ministries:

Ministry of Advanced Education
Ministry of Agriculture
Ministry of Central Services
Ministry of Education
Ministry of the Economy
Ministry of Environment
Executive Council
Ministry of Finance
Ministry of Government Relations
Ministry of Health
Ministry of Highways and Infrastructure
Ministry of Justice
Ministry of Labour Relations and Workplace Safety
Ministry of Parks, Culture and Sport
Public Service Commission
Ministry of Social Services

Treasury Board Agencies:

Apprenticeship and Trade Certification Commission
Financial and Consumer Affairs Authority
Global Transportation Hub Authority
Physician Recruitment Agency of Saskatchewan
Public Guardian and Trustee
Saskatchewan Legal Aid Commission
Saskatchewan Grain Car Corporation
Saskatchewan Housing Corporation
Water Security Agency

Other Agencies:

Technical Safety Authority of Saskatchewan

8.0 Glossary

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).

Change Management—An organized approach for introducing changes into a program or process, used to minimize unintended consequences.

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.

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

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.

9.0 Selected References

Canadian Institute of Chartered Accountants (CICA). (2009). *Trust Services Principles, Criteria, and Illustrations.* Toronto: Author.

International Organization for Standardization. (2005). ISO/IEC 270002:2005(E). *Information Technology – Code of Practice for Information Security Management; 2nd Edition*. Geneva: Author.

The Information Systems Audit and Control Association. (2012). *COBIT 5*. Rolling Meadows, IL: Author.