Chapter 11
Information Technology Office—Annual Security Audit

1.0 Main Points

The Information Technology Office (ITO) provides information technology (IT) services to 26 government ministries and agencies (clients). ITO has an agreement with a third-party service provider to operate and maintain a network and data centre on behalf of ITO. The data centre includes computers that host client systems and data. ITO needs to have effective controls and ensure its service provider follows effective security processes to protect client systems and data.

All organizations, including ITO, are subject to security threats including cyberattacks. ITO has worked with its service provider to improve data centre security. However, ITO needs to do more to protect systems and data, such as:

- Complete IT security standards for its clients
- Monitor whether the service provider meets all security requirements
- Provide relevant and timely security reports to clients
- Adequately restrict user access to client systems and data
- Adequately configure and update its server and network equipment
- Have a complete and tested disaster recovery plan for the data centre and clients' systems

Until ITO addresses the weaknesses we report in this chapter, systems and data are at an increased risk of loss, disclosure, or unauthorized modification and may not be available when needed.

2.0 Introduction

The Information Technology Office (ITO) of the Ministry of Central Services[1] delivers information technology (IT) to clients. Since 2005, ITO has entered into agreements with 26 clients to deliver IT services. The agreements cover 45,000 electronic assets (e.g., computers, printers) and 1,500 applications[2] that are used by over 12,000 client staff throughout the province. A complete list of clients as of March 31, 2013 is included in **Section 11.0**.

ITO's agreements with its clients make it responsible for providing secure IT services. To deliver its services to clients, ITO operated a data centre from 2005 until December 2010. In December 2010, ITO outsourced the data centre to a third-party service provider. ITO remains responsible for meeting the requirements it has agreed upon with clients.

[1] Effective May 25, 2012, the Information Technology Office became part of the Ministry of Central Services.
[2] *Information Technology Office Annual Report 2011-12*, p. 6.

In this chapter, we assess whether ITO has effective security processes to protect the confidentiality, integrity, and availability of information technology systems and data. We perform this audit annually to support our audits of ministries and other government agencies.

3.0 ITO's Relationship with its Service Provider

ITO has an agreement with its service provider to deliver data centre services for clients on ITO's behalf. The agreement sets out the roles and responsibilities of both ITO and its 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 telecommunications equipment that allows 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.

ITO and its service provider have agreed on how the data centre and all related equipment is to be configured, managed, and maintained. The service provider is required to annually report to ITO on 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 may not run properly with the latest server updates. ITO/clients need a plan for how to address these exemptions as they could pose a security risk in the future (see **Section 8.3**).

4.0 Services Provided Directly by ITO

ITO provides some services directly to clients. For example, ITO client service representatives manage the relationship between ITO and its clients. ITO also maintains a help desk that supports client requests. Help desk staff support client user access requests (e.g., granting/removing access to systems/data, password resets) and help resolve problems encountered by client staff.

ITO's security team monitors and follows up on security threats identified by security tools (e.g., firewalls). ITO staff also review and follow up on security information provided by its service provider.

5.0 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.[3] Organizations need effective

[3] 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/prg/ns/cybr-scrty/_fl/ccss-scc-eng.pdf (11 April 2013).

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. Saskatchewan is not immune to this threat; the Government of Saskatchewan can never fully protect itself 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, the importance of effective security processes cannot be understated.

To protect the security of systems and data, ITO needs to ensure 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.

6.0 Audit Objective

The objective of our audit was to assess whether the Information Technology Office of the Ministry of Central Services had effective processes to protect the confidentiality, integrity, and availability of information technology systems and data for the period from May 25, 2012 to March 31, 2013.[4]

7.0 Audit Scope, Criteria, and Conclusion

We examined both ITO's and its service provider's controls used to secure the data centre. We also examined ITO's agreements, minutes, reports, policies, and processes.

The audit did not assess the adequacy of security controls (e.g., user access controls) for specific client systems (e.g., financial accounting or payroll systems) or for computer equipment in use at client locations. We assess these controls in our audits of those ministries and other government agencies.

To conduct our audit, we followed the *Standards for Assurance Engagements* published in the *CICA 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.

[4] Effective May 25, 2012, the Information Technology Office became part of the Ministry of Central Services.

Figure 1—Audit Criteria

To have effective processes to protect the confidentiality, integrity, and availability of systems and data 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 Threat and risk assessments are performed
   - 1.3 Management approves security policies and procedures
   - 1.4 Management monitors security including its service provider
2. **Protect systems and data from unauthorized access**
   - 2.1 User access controls protect systems from unauthorized access
   - 2.2 Physical security controls protect the data centre from unauthorized access
3. **Ensure systems and data centre remain 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 systems and data**
   - 4.1 Change management processes exist and are followed
   - 4.2 Operational processes exist and are followed

We concluded that for the period from May 25, 2012 to March 31, 2013, ITO had effective controls to protect the confidentiality, integrity, and availability of systems and data except that ITO needs to:

- **Monitor whether its service provider meets all aspects of ITO's security requirements—ITO needs additional information from the service provider in the area of configuration management**
- **Restrict user access to systems and data—ITO does not consistently follow its processes for removing terminated users or fully comply with its password requirements**
- **Configure and update its server and network equipment to protect them from security threats—ITO has appropriately updated and configured certain key servers and network equipment, but it needs to fully secure all servers and network equipment**
- **Complete and test a disaster recovery plan for the data centre and client systems—ITO performs backups and keeps these offsite, but ITO does not have an approved and tested plan to recover systems and data in the event of a disaster**
- **Provide relevant and timely security reports to clients—ITO's reports to clients do not adequately inform clients whether ITO is securing their systems and data**
- **Complete security policies that set a minimum IT security standard for clients—ITO has its own established policies but it has not completed security policies for clients**

8.0 Key Findings And Recommendations

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

8.1 Need to Effectively Monitor Whether the Service Provider Meets its Security Requirements

We recommended that the Information Technology Office 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 to monitor its service provider did not significantly change during the audit period. ITO continues to have agreements with the service provider that outline security requirements for configuring and maintaining computer equipment. Management has processes that require it to meet regularly with its service provider. Management also receives monthly service-level reports (e.g., system availability statistics) and receives some security reports (e.g., security project status reports) periodically.

However, the reports that document the service provider's compliance with defined security requirements are not yet complete. ITO needs complete and timely reports to effectively monitor whether the service provider is meeting ITO's security requirements. For example, servers are not included in compliance reporting. As described in **Section 8.3**, we found weaknesses with configuration management. Without timely and complete information, ITO may not be able to take timely corrective action to resolve weaknesses.

ITO management advised us that it expects to receive complete security reports from its service provider in May 2013 and annually thereafter.

8.2 Need to Adequately Restrict User Access

We recommended that the Information Technology Office of the Ministry of Central Services adequately restrict access to systems and data. (2012 Report – Volume 2)

Status – Not Implemented

ITO did not significantly improve its processes for restricting user access during the audit period. ITO has documented processes for network user access management. However, as with past audits, ITO did not consistently follow its processes for removing network access for users who no longer require it on a timely basis.

ITO requires user identification accounts and passwords to access all systems and data. While most systems follow ITO policy requirements, some do not. ITO has currently exempted some user accounts from following its established standards. For example, some passwords for accounts do not expire. Weak password controls increase the possibility that a password may be compromised and used by an unauthorized person to gain system access.

8.3 Need to Adequately Configure and Update Server and Network Equipment

We recommended that the Information Technology Office 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)

Status – Partially Implemented

ITO is working with clients and its service provider to securely configure all servers. ITO has made some improvements during the audit period to increase the timeliness of server security updates. ITO's service provider now patches most servers that manage its network on at least a quarterly basis. However, patching on all servers is not yet complete for all known vulnerabilities.

ITO did not improve its firewall configurations during the audit period. As noted in our past reports, ITO requires firewalls to protect its data centre. The data centre firewalls are in appropriate locations and monitored. However, the data centre firewalls are not properly updated. Also, ITO's firewall rules do not effectively restrict data communications from accessing the data centre. The weakness is due to ITO not effectively defining the firewall rules that its service provider needs to follow. Without adequate firewall rules, the risk of a security breach increases. We also note continuing issues with updating and monitoring firewalls that protect client locations.

Without adequate configuration, someone could gain unauthorized access, obtain confidential information, inappropriately modify systems or data, or perform malicious acts that could affect availability.

8.4 Complete Disaster Recovery Plan Required

We recommended that the Information Technology Office 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 has identified the need to improve its disaster recovery processes. ITO wants to receive additional funding for a data centre contingency site, and would like to use a

contingency site to provide critical IT services to ITO and its clients in the event the primary data centre is unavailable for use.

ITO continues to work with its clients to define disaster recovery needs for critical applications. In some cases, ITO has helped clients contract for disaster recovery solutions for specific applications.

ITO does not have a complete and tested disaster recovery plan, but needs one to identify who is responsible for what. 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, when systems and data would be fully operational, or at what cost.

Neither ITO nor its clients know whether systems and data could be restored when needed in the event of a disaster. This could result in systems, data, and services being unavailable to the Government and the people of Saskatchewan.

8.5 Provide Relevant and Timely Security Reports to Clients

We recommended that the Information Technology Office 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

In **Section 8.1**, we note that ITO needs to effectively monitor its service provider. We also note that the service provider has agreed to periodically provide ITO with complete security reports that describe the service provider's compliance with agreed-upon requirements. In the same way, ITO's clients need information from ITO to enable them to monitor the services provided by ITO. ITO's clients need to know that ITO – their service provider – is doing its job. Our expectation is that ITO will provide its clients with timely and relevant security reports to allow effective monitoring.

During the audit period, ITO continued to provide risk assessment information to clients and periodically meet with staff at client agencies to discuss service issues and ongoing operations. However, during the audit period, ITO did not make significant improvements to the reports that it provides to its clients. The reports to clients do not outline ITO security controls in place or deficiencies with those controls. Accordingly, clients do not have adequate information on the potential impact that significant security weaknesses of ITO could have on their systems and data. Clients need this information to make decisions about how best to manage their systems and data.

8.6 Complete Client Security Policies Required

We recommended that the Information Technology Office 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 has not completed development of security policies and procedures that its clients need to follow.

Our expectation is that, to protect the security of its data centre, ITO needs to ensure its clients follow effective security policies and procedures. This is because a security weakness at a client poses risks to ITO and all of its clients.

ITO is working with its clients to classify their systems and data. Classification allows ITO and its clients to document system and data risks and helps define what security requirements are needed for each type of data (e.g., confidential). ITO expects the result of data classification by clients will help define client security policy requirements.

9.0 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 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.

10.0 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.

IT Governance Institute. (2007). *COBIT 4.1*. Rolling Meadows, IL: Author.

11.0 ITO Client List

Ministry of Advanced Education
Ministry of Agriculture
Ministry of Central Services
Ministry of Education
Ministry of the Economy
Ministry of Environment
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 Social Services
Ministry of Parks, Culture and Sport
Apprenticeship and Trade Certification Commission
Executive Council
Financial and Consumer Affairs Authority
Global Transportation Hub Authority
Office of the Provincial Capital Commission
Office of the Provincial Secretary
Physician Recruitment Agency of Saskatchewan
Saskatchewan Legal Aid Commission
Saskatchewan Grain Car Corporation
Saskatchewan Housing Corporation
Saskatchewan Municipal Board
Technical Safety Authority of Saskatchewan