Chapter 29
Information Technology Office—Annual Security Audit

1.0 Main Points

The Information Technology Office (ITO) provides IT services to over 30 clients. ITO has an agreement with a third party service provider to operate and maintain ITO's network and data centre. 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.

ITO needs to do more to protect client 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

Without effective central controls, there is greater risk of inappropriate access or changes to systems and data and greater risk that systems and data will not be available when needed.

Effective May 25, 2012, ITO became part of the Ministry of Central Services. As a result, the Ministry of Central Services became responsible for information technology for the Government of Saskatchewan.[1]

2.0 Introduction

ITO delivers information technology (IT) services to government ministries and agencies (clients). ITO buys, distributes, and manages IT hardware and software. ITO also develops IT applications, based on client requests, and provides project management services on IT projects.

ITO provides IT services to over 12,000 staff at 31 clients.[2] Its clients are primarily government ministries along with other government agencies. A complete list of clients as at February 29, 2012 is included in Section 10.0.

[1] *The Ministry of Central Services Regulations*, ss. 3(j),(k) and (l).
[2] ITO *Annual Report 2011-12*, p.6. Note that these numbers include ITO.

Clients rely on ITO to have effective controls and to carry them out properly. We perform this audit annually to support our audits of ministries and other government agencies that are ITO's clients.

3.0 Background

Information technology is an integral part of delivering many government programs and services. To deliver services effectively and achieve objectives, government agencies need to know that their IT systems and data are secure. That is, they need to know that processes are in place and are operating effectively to protect the confidentiality, integrity, and availability of their systems and data.

While ITO is a service provider to its clients, ITO itself has an agreement with a third party service provider to operate and maintain the network and data centre. The data centre is the central location for computer network hardware and software, and includes computers that host applications and store data. While ITO continues to carry out some IT services directly, including application development and managing user access, most data centre services are provided by ITO's service provider.

To protect the security of client systems and data, ITO needs to ensure its service provider follows effective security processes and that ITO's clients follow minimum security requirements. This is because a weakness involving the service provider or at a client location poses risks to ITO and all clients.

4.0 Audit Objective

The objective of our audit was to assess whether ITO had effective controls to protect the confidentiality, integrity, and availability of client information technology systems and data for the six-month period from September 1, 2011 to February 29, 2012.

5.0 Audit Scope and Criteria

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

We followed the *Standards for Assurance Engagements* published in the *CICA Handbook-Assurance*. To evaluate ITO's processes, we used criteria based on the work of other auditors and literature listed in the selected references. The criteria are primarily based on the *Trust Services Criteria, Principles, and Illustrations* authored by The Canadian Institute of Chartered Accountants (CICA) and American Institute of Certified Public Accountants. ITO agreed with the criteria.

Figure 1—Audit Criteria

To have effective controls to protect the confidentiality, integrity, and availability of client information technology systems and data, ITO should:

1. **Demonstrate management commitment to security**
   - Have an adequate agreement with its service provider
   - Threat and risk assessments are performed
   - Management approves security policies and procedures
   - Management monitors security including its service provider
2. **Protect client systems and data from unauthorized access**
   - User access controls protect client systems from unauthorized access
   - Physical security controls protect the data centre from unauthorized access
3. **Ensure client systems and data centre remain available for operation**
   - System and data backups occur and are tested
   - Disaster recovery and business continuity plans are in place
4. **Ensure the integrity of client systems and data**
   - Change management processes exist and are followed
   - Operational processes exist and are followed

6.0 Audit Conclusion

We concluded that for the six-month period from September 1, 2011 to February 29, 2012, ITO had effective controls to protect the confidentiality, integrity, and availability of client information technology systems and data except that ITO needs to:

- **Complete 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**
- **Monitor whether the service provider meets all aspects of its security requirements—ITO needs additional information from the service provider in the areas of server management and disaster recovery capacity**
- **Provide relevant and timely security reports to its clients—ITO's reports to clients do not adequately inform clients whether ITO is securing their systems and data**
- **Adequately restrict user access to client systems and data—ITO does not consistently follow its processes for removing access of former employees or fully comply with its password requirements**
- **Adequately 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**
- **Have a complete and tested 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**

Recommendations previously directed at ITO are now directed at the Ministry of Central Services consistent with the new legislative mandate of the Ministry of Central Services.

7.0 KEY FINDINGS AND RECOMMENDATIONS

7.1 Define Service Provider Requirements

We recommended that the Information Technology Office finalize defining the security requirements its service provider needs to follow. (2011 Report – Volume 2; Public Accounts Committee agreement June 25, 2012)

Status – Implemented (except for specifying disaster recovery services).

Our expectation is that the service provider agreement should include security requirements for configuring and maintaining computer equipment. The agreement should also define expected availability requirements including specific backup and disaster recovery requirements.

During the audit period, ITO and the service provider defined configuration and maintenance requirements for all computer and network equipment. ITO plans to review these requirements annually. ITO and its service provider have not yet agreed upon disaster recovery services. We discuss this weakness in Sections 7.3 and 7.8.

7.2 Complete Client Security Policies Required

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

Status – We continue to make this recommendation.

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 processes. This is because a security weakness at a client poses risks to ITO and all its clients.

Strong security starts with both ITO and clients agreeing on the security requirements that client staff need to follow. ITO and its clients are developing security policies and procedures based on international standards. A working group that includes ITO and client representatives met periodically to discuss needs and review draft policies. During the year, the working group approved new policies and procedures. However, at February 29, 2012, the work was not complete. For example, ITO was still working with clients to develop a data protection policy and a policy regarding responsibility for assets policy. Without complete policies and procedures, expectations may not be clear

and assessments of whether clients are following the security controls cannot take place.

7.3 Monitor Whether the Service Provider Meets All Aspects of Agreed Upon Requirements

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

Status – We continue to make this recommendation.

ITO did not receive complete reporting on all key equipment or on its service provider's disaster recovery capacity.

Our expectation is that ITO will monitor its service provider to make sure the service provider is providing the services as agreed upon. Appropriate monitoring includes the receipt and timely review of security compliance and service level reports provided by the service provider. ITO needs complete reports to effectively monitor whether the service provider is meeting ITO's security requirements. Monitoring also includes periodically meeting with the service provider to discuss issues and evaluate whether the contractual requirements are being met. Appropriate monitoring would enable ITO to take timely corrective action to resolve weaknesses.

Senior management of ITO and the service provider met periodically during the year to discuss the services provided. Management staff also met regularly to discuss operational issues.

The service provider's reporting improved during the year. ITO now receives monthly reports from the service provider. The reports included information on system availability and service level statistics such as the number of work orders requested and completed. The service provider also provided ITO with periodic reports on compliance with specific security requirements.

The service provider's reports need further improvement. The security compliance reports received from the service provider did not address all key equipment. For example, servers are not included in compliance reporting. Also, ITO did not receive any reports on the service provider's disaster recovery capacity. As described later in this chapter, we found significant weaknesses with both server management and disaster recovery planning.

7.4 Provide Relevant and Timely Security Reports to Clients

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

Status – We continue to make this recommendation.

ITO does not provide clients with adequate information on the operating effectiveness of its controls.

In Section 7.3, we note that ITO needs to effectively monitor its service provider. 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 year, ITO continued to periodically meet with staff at client agencies to discuss service issues and ongoing operations. ITO also continued to provide risk assessment information to clients. However, ITO has not made 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.

7.5 Protect Systems and Data from Security Threats

We recommended the Information Technology Office protect its systems and data from security threats. (2006 Report – Volume 3; Public Accounts Committee agreement April 3, 2007)

Status – Weaknesses relating to access and managing key network and server equipment continue to exist. We have updated our reporting and recommendations in Sections 7.6 and 7.7 to more clearly describe the remaining weaknesses.

Securing client systems and data requires strong controls. This includes strong central controls, such as at the data centre. Without strong data centre controls, someone could gain unauthorized access, obtain confidential information, inappropriately modify systems or data, or perform malicious acts that could affect availability.

ITO's data centre includes several layers of controls designed to prevent unauthorized access. While many of these controls work effectively, some do not. ITO needs to

improve its controls related to restricting access and managing key equipment. ITO has not made improvements to these controls during the audit period. The security controls required are generally accepted security practices for every data centre.

7.6 Adequately Restrict Access to Client Systems and Data

User access management controls should restrict access to authorized individuals and enforce strong password controls. ITO has documented processes for user access management. However, as with past audits, ITO did not consistently follow its processes for removing access for terminated users on a timely basis. Nor did it always enforce adequate password controls. For example, some passwords for network 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.

1. **We recommend that the Information Technology Office of the Ministry of Central Services adequately restrict access to client systems and data.**

7.7 Adequately Configure and Update Server and Network Equipment

Network infrastructure supports communications between client locations and the data centre. Network infrastructure needs effective security controls to prevent unauthorized people from communicating with computers inside the data centre. The network infrastructure should also ensure communications between locations are secure.

Protecting data transmitted between the data centre and client locations requires a secure communications network or strong encryption processes. Highly confidential data may require both. As noted in our past reports, neither ITO nor its clients know whether the security controls in the existing network (CommunityNet) are adequate to meet their needs. Nor do ITO and its clients always encrypt confidential data.

The first layer of network infrastructure security is a firewall. A firewall decides whether to allow or block incoming and outgoing communications to the data centre. For example, a firewall policy would allow staff at the Ministry of Social Services head office to send communications to the data centre but should have other rules restricting data communications with other locations (e.g., foreign nations).

As noted in our past reports, ITO has implemented firewalls to protect its data centre. The network firewalls are in appropriate locations, updated, and monitored. However, the firewall policies need updating. Without adequate firewall policies, the risk of unauthorized access increases. We also note continuing issues with updating and monitoring firewalls that protect client locations.

Servers are computers that run applications and store client data. Properly secured servers restrict access to authorized users and receive timely updates for known

security threats. ITO and the service provider have agreed-upon secure server configurations. However, consistent with previous audits, the agreed-upon configurations are not yet implemented. Also, some servers did not receive timely updates against known security threats during the audit period.

2. We recommend 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.

7.8 Complete Disaster Recovery Plan Required

We recommended the Information Technology Office 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 does not have a complete and tested disaster recovery plan.

A disaster recovery plan defines staff responsibilities and documents systems recovery processes. Our expectation is that ITO have an approved and tested disaster recovery plan.

Consistent with our past audits, ITO does not have a complete disaster recovery plan. ITO needs a complete plan that identifies who is responsible for what. ITO currently uses a service provider for the data centre. ITO's disaster recovery plan should accordingly set out responsibilities for both its staff and those of its service provider.

ITO's disaster recovery plan does not address client requirements for recovery of their systems and data. Clients rely on their systems and data to run their operations. If client systems become unavailable, client operations may be impaired or stopped completely. Currently, neither ITO nor 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.

8.0 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).

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.

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

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.

IT infrastructure—An organization's computer and network assets.

Network—A group of computers that communicate with each other.

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.

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

10.0 ITO Client List

As of February 29, 2012

Ministry of Advanced Education, Employment and Immigration
Ministry of Agriculture
Ministry of Corrections, Public Safety and Policing
Ministry of Education
Ministry of Energy and Resources
Ministry of Environment
Ministry of Finance
Ministry of First Nations and Métis Relations
Ministry of Government Services
Ministry of Health
Ministry of Highways and Infrastructure
Ministry of Justice and Attorney General
Ministry of Labour Relations and Workplace Safety
Ministry of Municipal Affairs
Public Service Commission
Ministry of Social Services
Ministry of Tourism, Parks, Culture and Sport
Apprenticeship and Trade Certification Commission
Enterprise Saskatchewan
Executive Council
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 Financial Services Commission
Saskatchewan Grain Car Corporation
Saskatchewan Housing Corporation
Saskatchewan Municipal Board
Technical Safety Authority of Saskatchewan