Information Technology Office

16

Main points

The Information Technology Office (ITO) complied with the authorities governing its activities relating to financial reporting, safeguarding public resources, revenue raising, spending, borrowing, and investing.

As a custodian of ministries' information systems and data, the ITO must protect the confidentiality, integrity, and availability of ministry information technology (IT) systems and data. ITO had adequate procedures to safeguard public resources with the exception of the following.

To protect ministry IT systems and data, ITO needs to:

- define security requirements its service provider needs to follow
- monitor whether its service provider meets its security requirements
- provide relevant and timely security reports to its clients
- complete policies that set IT security standards for clients
- protect systems and data from security threats
- have a complete and tested disaster recovery plan for the data centre and client systems

ITO needs to follow its processes to ensure that ITO user access is removed in a timely way. ITO should sign adequate agreements with ministries before delivering services to them, ensure agreements address security and disaster recovery requirements, and improve its human resource plan.

This chapter also contains an update on the status of previous recommendations agreed to by the Standing Committee on Public Accounts.

Introduction

The mandate of Information Technology Office (ITO) includes: "to develop, promote, and implement policies and programs of the Government of Saskatchewan relating to information technology and information management."[1]

For further details regarding ITO's mandate and operations, consult its publications on its website at www.ito.gov.sk.ca.

Financial overview

The following is a list of major programs and spending:

	Original Estimates[2]	Actual[3]
	(in millions of dollars)	
Central Management and Services	$ 2.1	$ 2.9
IT Coordination and Transformation Initiatives	5.3	4.7
Application Administration and Support	8.7	9.1
Interministerial Services	--	0.3
	16.1	17.0
Major Capital Asset Acquisitions	2.3	1.6
	$ 18.4	$ 18.6

ITO provides information technology (IT) services to client ministries on a cost recovery basis. The total amount recovered from client ministries for 2010-11 was $75.3 million.

Audit conclusion and findings

In our opinion, for the year ended March 31, 2011:

- **ITO had adequate rules and procedures to safeguard public resources except for the matters described in this chapter**

[1] *The Information Technology Office Regulations, 2007*, s. 3(b).
[2] Information Technology Office, *2010-11 Annual Report*, p. 21. www.ito.gov.sk.ca
[3] Ibid., p. 21.

- **ITO complied with the following authorities governing its activities relating to financial reporting, safeguarding public resources, revenue raising, spending, borrowing, and investing:**

  The Economic and Co-operative Development Act **(sections 8(c), 9(1)(h), and 9(3))**
  The Government Organization Act
  The Information Technology Office Regulations
  The Information Technology Office Service Regulations
  The Public Works and Services Act **(sections 4(2)(j) and (n))**
  The Public Service Act, 1998
  The Financial Administration Act**, 1993**
  Regulations and Orders in Council issued pursuant to the above legislation

In this chapter, we also report the results of our ITO security audit and provide an update on the status of previous recommendations agreed to by the Standing Committee on Public Accounts (PAC).

User access

ITO has adequate procedures for removing user access to its computer systems and data. However, ITO did not follow its established procedures. During the audit, we found 3 out of 17 individuals tested did not have their access removed on a timely basis. If former employees do not have access removed on a timely basis, it increases the risk of inappropriate access to ITO's systems and data.

As a result of this weakness, ITO's systems and data are at risk of inappropriate access.

1. **We recommend that the Information Technology Office follow its established procedures for removing user access to its computer systems and data.**

Exhibit 1—Status of past recommendations

Past recommendation (initial report)	Public Accounts Committee (PAC)	Update for 2010-11	Status of recommendation at March 31, 2011
We recommended that the Information Technology Office sign service level agreements with its clients prior to delivering information technology services. (2005 Report – Volume 3)	PAC agreed with this recommendation on May 16, 2006.	ITO is in the process of signing new agreements.	**Partially implemented** – we continue to make this recommendation.
We recommended that the Information Technology Office sign agreements with its clients on security and disaster recovery processes, expectations, and reporting requirements. (2005 Report – Volume 3)	PAC agreed with this recommendation on May 16, 2006.	ITO is in the process of signing new agreements. The agreements will require the ministries to purchase adequate disaster recovery from ITO.	**Partially implemented** – we continue to make this recommendation.
We recommended that the Information Technology Office's human resource plan: ***- quantify its future human resource needs*** ***- provide details on the human resource gap between actual and required resources*** ***- provide measurable indicators and targets for its key strategies*** ***- provide details on plans to implement the major strategies*** (2008 Report – Volume 3)	PAC agreed with this recommendation on December 10, 2008.	ITO has a Workforce Plan that quantifies its future human resources needs and provides details on the human resources gap between actual and required resources. ITO is in the process of developing a new Human Resources Plan with the help of the Public Service Commission.	**Partially implemented** – we continue to make this recommendation.
We recommended that the Information Technology Office prepare accurate and complete year-end financial reports as required by the Financial Administration Manual. (2010 Report – Volume 2)	PAC agreed with this recommendation on June 6, 2011.	ITO's March 31, 2011 financial reports contained significant errors. For example, its contractual obligations schedule had several incorrect amounts that resulted in an overall overstatement of contractual obligations by $3.3 million.	**Not implemented** – we continue to make this recommendation.

ITO security audit

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 26 clients who have over 12,000 employees.[4]

Effective December 6, 2010, ITO commenced an agreement with a service provider to operate and maintain its data centre until December 5, 2017. Under the agreement, ITO staff at the data centre became employees of the service provider. While ITO continues to carry out some IT services directly, including application development and user access, most data centre services are provided by a service provider.

Within the scope of the service agreement, ITO and the service provider agreed to develop a transition plan. The transition plan includes a set of project deliverables and milestones. Deliverables within the transition plan include transferring knowledge to the service provider and defining security controls for the service provider to implement.

The importance of IT security

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.

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

[4] ITO *2009-10 Annual Report*, p.8. Note that these numbers include ITO.

Audit objective and criteria

The objective of our audit was to assess whether ITO had adequate controls to protect the confidentiality, integrity, and availability of client information technology systems and data for the period from December 6, 2010 to March 6, 2011. We did not include clients' security controls in the scope of this audit.

We perform this audit every year. The results support our other audit work performed at ministries and other government agencies.

We used criteria to assess ITO's processes. The criteria are based on the *Trust Services Criteria, Principles, and Illustrations* authored by The Canadian Institute of Chartered Accountants (CICA) and the American Institute of Certified Public Accountants and international standards and literature. ITO agreed with the criteria.

Exhibit 2—Audit Criteria

1. Show management commitment to security
   - ITO has 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 are 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
   - Computer operation processes exist and are followed

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

Audit conclusion

We concluded that for the period from December 6, 2010 to March 6, 2011, the Information Technology Office had adequate controls to

protect the confidentiality, integrity, and availability of client information technology (IT) systems and data except it needs to:

- **define security requirements its service provider needs to follow**
- **monitor whether its service provider meets its security requirements**
- **provide relevant and timely security reports to its clients**
- **complete policies that set IT security standards for its clients**
- **protect systems and data from security threats**
- **have a disaster recovery plan for the data centre and client systems**

As described in the sections below, the recommendations identified in the prior years' audits continue to exist. While the service provider is now responsible for managing and maintaining the data centre, most processes in place prior to signing the agreement continued to exist during the current audit period. These processes will remain in place until ITO and its service provider agree upon and implement specific security requirements. In the interim, client systems and data remain at risk for loss or unauthorized disclosure.

In the section below, we describe the criteria in italics and set out our new and continuing findings and recommendations.

Key findings and recommendations by criterion

Show management commitment to security

We expected ITO to demonstrate commitment to security of client systems and data. Commitment includes outlining security requirements in an agreement with its service provider(s) and setting up a strong organizational structure that clearly defines who is responsible for monitoring security including the service provider. We expected IT threat and risk assessments would be performed. Commitment also includes implementing and monitoring compliance with security policies and

procedures. We expected ITO to report the adequacy of security and availability controls to clients on a timely basis.

ITO signed an agreement with a service provider effective December 6, 2010, for operating and maintaining its data centre. The agreement with the service provider does not include security requirements the service provider is to implement. ITO and its service provider agreed to document security requirements during a transition period.

As of March 6, 2011, ITO was in the process of agreeing on defining security requirements with its service provider. ITO should base the security requirements on a threat and risk assessment to ensure the security requirements will meet its clients' needs.

2. We recommend that the Information Technology Office finalize defining the security requirements its service provider needs to follow.

After defining security requirements, ITO then needs to monitor the service provider's compliance with the security requirements. The reporting to be provided from the service provider was also to be identified and agreed to during a transition period. However, as of March 6, 2011, ITO did not receive any reports on security from its service provider. Therefore, ITO is not able to assess whether the service provider is meeting its clients' security needs and properly securing the data centre.

3. We recommend that the Information Technology Office monitor whether its service provider meets its security requirements.

ITO has an appropriate IT organizational structure. Job descriptions set roles and responsibilities. ITO will need to update some job descriptions to reflect service delivery changes.

A member of senior management leads IT operations and members of senior management meet regularly with ITO's service provider. Senior management meets regularly to discuss IT operations and client issues.

We recommended that the Information Technology Office establish information technology security policies for its clients. *(2008 Report – Volume 3)*

PAC agreed with our recommendation December 10, 2008.

ITO's strategic plan defines key goals and objectives related to security. ITO adopted an IT security framework based on international standards to define respective roles and obligations of ITO and its clients. ITO and its clients are still developing and completing security policies and procedures within this framework. Until such policies and procedures are completed, ITO is unable to determine whether clients follow effective security controls.

Status – We continue to make this recommendation.

We recommended that the Information Technology Office provide relevant and timely security reports to its clients. *(2009 Report – Volume 3)*

PAC agreed with our recommendation June 18, 2010.

ITO has begun providing risk assessments to clients on proposed processes or equipment that do not meet ITO security requirements. Clients may choose to accept or mitigate the risks. ITO also meets regularly with its clients. It has set up, with its clients, a committee that meets to discuss security issues. ITO also provides reports to clients that describe potential security incidents that have occurred. However, ITO does not provide reports to clients that outline ITO security controls in place or deficiencies that occurred with those controls. Accordingly, clients do not have adequate information on the potential impact significant security weaknesses could have on their systems and data.

Status – We continue to make this recommendation.

Protect client systems and data from unauthorized access

We expected ITO to have adequate physical access and user access controls to protect client systems and data from unauthorized access.

Good physical access 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, ITO should physically prevent unauthorized persons from entering the 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. A client determines who should have access to its systems and data. The client then relies on ITO to make user access changes that it requests.

We expected ITO to monitor the service provider to ensure it was configuring, updating, and monitoring client systems against security threats. We also expected ITO to ensure secure data communications to and from the data centre.

The service provider has good physical access controls for protecting ITO's IT infrastructure at the data centre. It has several layers of physical access controls (e.g., locked and monitored doors) designed to prevent unauthorized persons from accessing the data centre.

We recommended that the Information Technology Office protect its systems and data from security threats. *(2006 Report – Volume 3)*

PAC agreed with our recommendation April 3, 2007.

ITO will continue to manage user access controls once the service provider transition is complete. ITO has adequate policies and procedures for granting and removing user access when requested by clients and for periodically reviewing access to systems and data. However, ITO needs to ensure it follows its process for removing user access on a timely basis. ITO has a process for identifying stale user accounts and reporting these accounts to clients. A user account is stale if it is not used for a

certain period (e.g., 45 days). Timely review of stale user accounts helps identify inappropriate user accounts (e.g., if a user is no longer employed).

ITO has adequate policies and procedures for enforcing use of passwords to access the network as well as for changing user passwords. However, ITO did not consistently follow its password requirements. For example, some passwords are not set to expire and ITO has no process for following up on such accounts.

In the prior year, ITO did not effectively configure or update its computer equipment. The service provider is now responsible for performing this work. However, the requirements of the service provider are not yet defined. As a result, the weaknesses identified in prior audits continue to exist. We found that servers were not updated during the audit period. Also, firewall and server configuration weaknesses are not resolved. Without appropriate security, unauthorized individuals may obtain access to systems and data without physically accessing restricted areas.

ITO and its clients need to protect the security of data transmitted between client locations and the data centre. The primary method used to transmit information is CommunityNet, a high-speed, province-wide data communication network.[5] Private and confidential government information travels over CommunityNet.

To protect data transmissions requires either a separate secure communications network or strong encryption processes. Highly confidential data may require both. A secure network has security controls that are tested and monitored for effectiveness. Neither ITO nor its clients know whether the security controls in CommunityNet are adequate to meet their needs. Nor do they always encrypt confidential data.

Status – We continue to make this recommendation.

Ensure client systems and data are available for operation

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

[5] SaskTel provides this network.

The availability of client systems and data requires effective backup and recovery processes. We expected ITO to have effective disaster recovery processes to ensure the data centre can be restored if a major problem occurs. Clients need to identify their disaster recovery requirements to ensure ITO can develop adequate plans to restore their systems.

The service provider performs daily data backups. The service provider has procedures for identifying backup failures and for transferring backup tapes to off-site storage. Off-site data backups help prevent data loss if the data centre is destroyed. However, backup data was not taken off-site on a daily basis during the audit period.

We recommended that the Information Technology Office have a disaster recovery plan for the data centre and client systems. *(2006 Report – Volume 3)*

PAC agreed with our recommendation April 7, 2007.

ITO has developed and approved a business continuity plan for ITO as well as a disaster recovery plan for the data centre. The disaster recovery plan defines who can activate the plan, identifies staff roles and responsibilities, and includes documentation on systems and recovery processes. ITO needs to update its plans to reflect the service provider.

ITO's disaster recovery plan does not adequately address client requirements for recovery of their systems and data. Neither ITO nor clients know whether systems and data can 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. ITO continues ranking recovery priorities among client systems in consultation with its clients.

ITO performed no testing of its disaster recovery plan in 2010 and up to March 6, 2011. ITO needs to test a disaster recovery plan to ensure it will work in the event of a disaster. ITO told us it plans to work with service providers to address disaster recovery requirements.

Status – We continue to make this recommendation.

Ensure the integrity of client systems and data

We expected ITO to have processes for maintaining the integrity of client systems and data by implementing strong change management and IT operation processes. The processes should include approval and testing of changes before implementation.

ITO has adequate change management policies and procedures. Policies and procedures include documenting, testing, approving, and moving changes from the test environment to operations. ITO has a change management committee that meets regularly to review and approve changes. However, ITO did not consistently follow its documented requirements. For example, management should document, for all significant changes, what to do if the change has unintended consequences (e.g., system failure). ITO needs to consistently follow its change management policies and procedures to protect its systems and data. We included this weakness as part of the protect systems and data from security risks recommendation described earlier in this chapter.

Computer operating processes help ensure that systems and data are secure and that only authorized users have access. We described our findings for these processes earlier in this chapter.

Selected references

Canadian Institute of Chartered Accountants (CICA). (2009). *Trust services principles, criteria, and illustrations*. 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. (2007). *COBIT 4.1*. Rolling Meadows, IL: Author.

Status of previous recommendations of the Standing Committee on Public Accounts

The following exhibit provides an update on recommendations agreed to by PAC, that are not yet implemented and are not discussed earlier in this chapter.[6] Our intent is to follow up outstanding recommendations in upcoming reports.

PAC REPORT YEAR[7]	OUTSTANDING RECOMMENDATION	STATUS
Information Technology Office—Benefit realization (2009 Report – Volume 1)		
2011	7-2 that the Information Technology Office work with ministries to prepare joint actions plans to address issues identified in satisfaction surveys, as required by its service level agreements.	**Partially implemented** (as at March 31, 2011).
2011	7-5 that the Information Technology Office seek mutual agreement with ministries on relevant service delivery measures and targets.	**Partially implemented** (as at March 31, 2011).

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).

Business continuity plan—A plan for an organization to carry on providing key programs and services after a serious disruption or emergency. The part of a business continuity plan that relates to

[6] For the definitions of key terms used in the exhibit, see Chapter 27 – Standing Committee on Public Accounts.
[7] PAC Report Year refers to the year that PAC first made the recommendation in its report to the Legislative Assembly.

restoring IT systems and data is often called a disaster recovery plan.

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.

IT security framework—An overall approach to IT security that includes and organizes more specific policies and procedures.

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.