Information Technology Office

13

Main points

As a service provider and custodian of ministry information systems and data, the Information Technology Office (ITO) must protect the confidentiality, integrity, and availability of ministry information technology (IT) systems and data.

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

- provide relevant and timely security reports
- establish policies that set a minimum IT security standard for ministries
- protect systems and data from security threats
- have a disaster recovery plan for its data centre and ministry systems

ITO needs to prepare accurate and complete financial reports. Also, ITO exceeded its appropriation by $5.1 million without obtaining a special warrant to authorize the additional spending. In addition, 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.

Introduction

The Information Technology Office Regulations, 2007 continues the Information Technology Office (ITO) as a ministry. The mandate of 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 ITO's major programs and spending:

	Original Estimates[2]	Actual[3]
	(in millions of dollars)	
Central Management and Services	$ 2.1	$ 2.1
IT Coordination and Transformation Initiatives	5.0	4.6
Interministerial Services	--	5.1
	7.1	11.8
Major Capital Asset Acquisitions	0.2	0.6
	7.3	12.4

ITO provides information technology (IT) services to client ministries on a cost recovery basis. The total amount recovered from client ministries for 2009-10 was $48.6 million (for core services provided), which was $5.1 million less than estimated.

[1] *The Information Technology Office Regulations, 2007*, s. 3(b).
[2] Saskatchewan Finance, *2009-2010 Saskatchewan Estimates.*
[3] Information Technology Office, *2009-2010 Annual Report.* www.ito.gov.sk.ca

Audit conclusions and findings

In our opinion, for the year ended March 31, 2010:

- **ITO had adequate rules and procedures to safeguard public resources except for the matters described in this chapter**
- **ITO complied with authorities governing its activities relating to financial reporting, safeguarding public resources, revenue raising, spending, borrowing, and investing except for the matter described in this chapter**

In this chapter, we also report the results of our ITO security audit and provide an update on recommendations previously made by the Standing Committee on Public Accounts (PAC) that are not yet implemented and have not been discussed elsewhere in this chapter.

Prepare accurate and complete financial reports

The *Financial Administration Manual (*FAM) requires ITO to give the Ministry of Finance a year-end financial report that shows the revenues, expenses, assets, and liabilities of ITO. The Ministry of Finance uses this report to prepare the financial statements of the General Revenue Fund.

ITO's financial reports for the year ended March 31, 2010 contained several errors. For example, its contractual obligations schedule had several incorrect amounts that resulted in an overall understatement of contractual obligations by $5.5 million.

1. We recommend that the Information Technology Office prepare accurate and complete year-end financial reports as required by the *Financial Administration Manual.*

Approved appropriation exceeded

ITO did not comply with the law as it incurred $5.1 million of spending without proper authority. This spending occurred as a result of not recovering all expenses for providing services to other ministries.

The Legislative Assembly, through appropriation acts, provides authority to ministries to spend money out of the General Revenue Fund. Under *The Financial Administration Act, 1993*, Cabinet can authorize further spending under certain circumstances. Such authorization is called a "special warrant."

For the year ending March 31, 2010, the Assembly authorized ITO to spend $7.3 million. ITO, however, spent $12.4 million during the year. ITO did not request or obtain a special warrant to authorize the additional spending of $5.1 million. As a result, ITO spent $5.1 million without proper authority.

ITO security audit

The mandate of ITO includes "to develop, procure and provide goods and services related to information technology and information management on behalf of the Government of Saskatchewan and to charge ministries for those goods and services." [4]

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

ITO states that it provides IT services to over 12,000 staff at 26 clients[5] of which the majority are ministries.

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.

[4] *The Information Technology Office Regulations, 2007*, s. 3(c).
[5] ITO *Annual Report 2008-09*, p.6. Note that these numbers include ITO.

ITO stores client data and computer equipment needed to run client systems in a data centre.[6] ITO also manages network equipment at client locations. ITO must manage the security risks associated with the data centre and network. It must also know whether security risks are managed at client locations and whether clients are meeting their security responsibilities. This is because a weakness at a client location poses risks to all users of ITO's services.

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 six-month period from September 1, 2009 to February 28, 2010.

We do this audit every year and use the results of this audit to support our other audit work performed at client agencies.

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

Exhibit—Audit Criteria

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

1. **Show management commitment to security**
   - Responsibility for security is clearly defined
   - Threat and risk assessments have been performed
   - IT planning supports security
   - Management has approved security policies and procedures
   - Management monitors security for the data centre and clients
2. **Protect client systems and data from unauthorized access**
   - User access controls protect the 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

[6] ITO uses one main data centre. It has additional data centres that it uses for testing and backup purposes.

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

While this audit focused on ITO's controls, adequate security requires that both ITO and clients have strong security controls. For example, clients need good physical security processes to ensure only authorized users have access to their systems and data. We did not include client security controls in the scope of this audit. However, we are aware of security weaknesses at some clients. For example, not all clients inform ITO to remove access for individuals who are no longer employed. Unless both ITO and its clients have strong security processes, client systems and data are at risk.

Audit conclusion

The Information Technology Office had adequate controls to protect the confidentiality, integrity, and availability of client information technology (IT) systems and data for the period from September 1, 2009 to February 28, 2010, except it needs to:

- **provide relevant and timely security reports to its clients**
- **establish policies that set a minimum IT security standard for clients**
- **protect systems and data from security threats**
- **have a disaster recovery plan for its data centre and client systems**

ITO told us that it plans to contract with external service providers for operation of its data centre. ITO told us it expects the change will assist it in responding to our security recommendations.

In the sections below, we describe the criteria in italics and set out our key 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 setting up a strong organizational structure that clearly defines who is responsible for security. A member of senior management leads a strong IT division. A steering committee ensures the IT division meets client needs. IT planning supports security, and threat and risk assessments have been performed that support the planning. The adequacy of security and availability controls is reported to clients on a timely basis. Commitment also includes implementing and monitoring compliance with security policies and procedures.

ITO has an appropriate IT organizational structure for securing its data centre. A member of senior management leads IT operations. Senior management meets regularly to discuss IT operations and client issues.

ITO's strategic plan defines key goals and objectives related to security. ITO uses an IT security framework based on international standards to protect its data centre. It continues to implement policies and procedures within this framework.

ITO did assessments and received security reports from independent reviews. Senior management received the results of this work. The work performed at ITO confirms that security weaknesses exist.

ITO improved its reporting to clients regarding security during the audit period. ITO meets regularly with its clients. It has set up, with its clients, a committee that meets to discuss security issues. ITO also provides service reports to clients that describe security incidents. However, ITO does not provide adequate information on its security weaknesses to clients or explain the potential impact of its weaknesses on client systems and data.

We continue to recommend that the Information Technology Office provide relevant and timely security reports to its clients. We reported this

matter in our 2009 Report – Volume 3. On June 18, 2010, PAC agreed with the recommendation.

ITO has agreements with most, but not all, of its clients. During the audit period, ITO began negotiating new agreements with its clients. The existing agreements require ITO and clients to jointly protect assets according to ITO's security framework.

During the audit period, ITO worked with its clients to revise the security framework. The new framework is intended to provide increased information on the respective roles and obligations of ITO and its clients. ITO and its clients are developing specific guidance in terms of the minimum security procedures clients must follow.

Accordingly, we continue to recommend that the Information Technology Office establish information technology security policies for its clients. We first reported this matter in our 2008 Report – Volume 3. On December 10, 2008, PAC agreed with the 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 its data centre.

User access controls ensure only approved people or processes can use an IT system. A common example of a user access control is a username and a password. The username identifies the user and the password grants access. 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 protect the data centre by configuring, updating, and monitoring its systems against security threats. We also expected ITO to secure data communications to and from the data centre.

ITO has good physical access controls for protecting its IT infrastructure. It has several layers of physical access controls designed to prevent unauthorized persons from accessing its data centre. ITO also has video surveillance processes for monitoring high security areas.

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. 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 do not expire.

ITO has adequate policies and procedures for updating its computers. ITO uses a formal threat and risk assessment to evaluate and rank security updates. However, ITO did not consistently follow its policies and procedures. For example, we found that ITO did not update its servers on a timely basis for known security threats.

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.[7] 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.

[7] CommunityNet is a data network provided by SaskTel.

ITO monitors two firewalls and an intrusion detection system at the data centre. This helps ITO detect inappropriate activity on its network on a timely basis. However, ITO needs to properly configure the firewalls to prevent unauthorized access to its network.

ITO also manages firewalls at client locations. ITO needs to properly configure the client firewalls and monitor them.

We continue to recommend that the Information Technology Office protect its systems and data from security threats. We first reported this matter in our 2006 Report – Volume 3. On April 3, 2007, PAC agreed with the 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.

Even with good backup and recovery procedures, an agency may not be able to continue its operations if a major problem occurs. Therefore, agencies should have strong contingency plans to recover operations in the event of a disaster like a fire or flood. This includes building capacity into systems, when cost effective, so a disaster in one location will not cause applications to quit running at other locations where employees are still able to work.

The availability of client systems and data requires strong processes at both ITO and clients. ITO needs to have processes to ensure it can restore its data centre. Clients need to identify their disaster recovery requirements to ensure ITO can develop adequate plans to restore their systems.

ITO performs daily data backups. ITO 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, ITO needs to follow all of its back-up processes. For example, ITO did not consistently transfer its backup data off-site on a daily basis.

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'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 told us it has begun to identify recovery priorities among client systems in consultation with its clients.

ITO has performed limited testing of its disaster recovery plan. Testing has relied on assumptions, such as equipment being available, that may not be valid in a disaster. ITO needs to test its disaster recovery plan to ensure it will work in the event of a disaster.

We continue to recommend that the Information Technology Office have a disaster recovery plan for its data centre and client systems. We first reported this matter in our 2006 Report – Volume 3. On April 3, 2007, PAC agreed with the 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. These 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.

Computer operating processes help ensure that systems and data are secure, that only authorized users have access, and that computers are kept up to date. We describe our findings for these processes earlier in this chapter.

Selected references

Canadian Institute of Chartered Accountants and American Institute of Certified Public Accountants. (2009). *Trust Services Principles, Criteria, and Illustrations*. New York: Author.

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

International Organization for Standardization. (2005). ISO/IEC 17799:2005(E). *Information technology – Code of practice for information security management; 2nd Edition*. Geneva: Author.

The Information Systems Audit and Control Foundation. (2005). *CoBiT-governance, control and audit for information and related technology; 4th Edition*. Rolling Meadows, IL: Author.

Status of outstanding recommendations of the Standing Committee on Public Accounts

The table below provides an update on recommendations previously made by PAC, that are not yet implemented and are not discussed earlier in this chapter.[8]

PAC REPORT YEAR[9]	OUTSTANDING RECOMMENDATION	STATUS
Information Technology Office		
2007	PAC concurs: 8-1 that the Information Technology Office should sign service level agreements with its clients prior to delivering information technology services.	**Partially implemented** (as at March 31, 2010). ITO is in the process of signing new agreements.
2007	PAC concurs: 8-2 that the Information Technology Office should sign agreements with its clients on security and disaster recovery processes, expectations, and reporting requirements.	**Partially implemented** (as at March 31, 2010). ITO is in the process of signing new agreements. The agreements will require the ministries to purchase adequate disaster recovery processes.
2009	PAC concurs: 12-1 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	**Partially implemented** (as at March 31, 2010). ITO produced a Workplace Plan that quantifies its future human resources needs and provides details on the human resources gap between actual and required resources.

[8] For the definitions of key terms used in the table, see Chapter 24 – Standing Committee on Public Accounts.
[9] PAC Report Year refers to the year that PAC first made the recommendation in its report to the Legislative Assembly.

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 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.

Intrusion detection system (IDS)—Software and/or hardware designed to detect a security breach by identifying inappropriate access or changes taking place within a computer or network.

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.

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.