Information Technology Office

12

Main points

The Information Technology Office (ITO) provides information technology (IT) services to client ministries. ITO needs to improve its human resource plan to help ensure it has the right people, in the right jobs, at the right time.

As a service provider and custodian of client information systems and data, ITO must protect the confidentiality, integrity, and availability of client IT systems and data. ITO has adequate controls to protect client IT systems and data except ITO needs to:

- establish information security policies for its clients
- protect its systems and data from security threats
- implement a disaster recovery plan for its data centre and client systems

We also followed up our earlier audit of ITO's processes to manage the delivery of agreed-upon services to clients. We continue to recommend that ITO work with its clients to implement agreements that govern service delivery, security, and disaster recovery. We continue to recommend that ITO sign adequate agreements with its clients before delivering services to them.

Introduction

The Information Technology Office Regulations established 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 at its website at www.ito.gov.sk.ca/.

Financial overview

The following is a list of ITO's major programs and spending including capital acquisitions. For further detail, see ITO's 2007-2008 Annual Report available on its website.

	Estimates[2]	Actual
	(in thousands of dollars)	
Central Management and Services	$ 1,925	$ 1,771
IT Coordination and Transformation Initiatives	3,113	3,574
Major Capital Asset Acquisitions	250	0
Inter-ministerial Services	0	44
	$ 5,288	$ 5,389

ITO provides IT services to client ministries on a cost recovery basis. The total billed to client ministries for 2007-08 was approximately $55.6 million.

Audit conclusions and findings

In our opinion for the year ended March 31, 2008:

- **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] Saskatchewan Finance, *2007-2008 Saskatchewan Estimates*. The Estimates total does not include the additional $240,000 authorized through the *Saskatchewan Supplementary Estimates* for ITO (Vote 74).

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

In this chapter, we also report the results of our ITO security audit and follow up on our past recommendations related to managing IT service delivery.

Improvements to human resource plan needed

ITO needs to improve its human resource plan to ensure it has the right people, in the right jobs, at the right time.

In 2007-08, ITO developed its *Information Technology Office HR Plan 2008-09.* We assessed this plan against the key elements of a human resource plan.

A good human resource plan needs to set priorities and link to the agency's overall strategic direction. It should also identify key human resource risks and gaps that exist in current and future available resources. The plan should also set out strategies and implementation plans to address human resource risks and gaps.

We found that ITO's human resource plan sets priorities and identifies key human resource risks. The plan sets out its current supply of human resources but does not provide any information on the future supply of human resource needs. Therefore, the plan does not describe the gap that exists between required and actual human resources.

The plan sets out strategies and broad action plans to address the human resource risks identified. However, it does not provide completion dates or assign responsibility for carrying out the action. The plan should also describe how ITO would monitor the implementation of the major strategies and achievement of planned results. Measurable indicators and targets were not set out in the plan for its key strategies to help ITO monitor its progress.

1. **We recommend 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

Management told us that ITO has had significant growth and changes in staff due to the consolidation of government information technology (IT) services and that it is working on addressing its human resource needs.

ITO security audit

Providing information technology services to clients

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."[3]

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

ITO states that it provides IT services to 20 government ministries and agencies, including more than 9,000 government employees.[4]

The importance of 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.

[3] *The Information Technology Office Regulations, 2007*, s. 3(c).
[4] www.ito.gov.sk.ca/consolidation (April 17, 2008).

ITO stores client data as well as hardware and software necessary to run client systems in a data centre.[5] 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 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 period September 1, 2007 to February 29, 2008.[6]

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 and the American Institute of Certified Public Accountants and on international standards, literature, and reports of other legislative auditors. ITO agreed with the criteria.

The criteria, set out in the exhibit below, describe the key processes that we expected ITO to use to secure client systems and data.

[5] Our work focused on ITO's main data centre. ITO has additional data centres that it uses for testing and backup purposes.

[6] Our Office performed similar audits for earlier periods. These are reported in Chapter 6 of our 2006 Report—Volume 3, and Chapter 14 of our 2007 Report—Volume 3.

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

Throughout our audit, we followed *The Standards for Assurance Engagements* established by The Canadian Institute of Chartered Accountants.

While this audit focused on ITO's controls, adequate security requires that clients also 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 to 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 systems and data for the period September 1, 2007 to February 29, 2008 except it needs to:

- **establish information technology security policies for its clients**
- **protect its systems and data from security threats**
- **have a disaster recovery plan for its data centre and client systems**

Key findings by criterion

Show management commitment to security

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. It has a steering committee to ensure the IT division meets client needs. Commitment also includes implementing and monitoring compliance with security policies and procedures.

ITO has an effective 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 has set up processes for integrating new clients that join it. ITO meets regularly with its clients.

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 risk assessments and received security reports from independent reviews. It also did quality assurance tests internally. For example, ITO tested user access processes during the audit period. Senior management receives information on quality assurance results.

ITO does not have agreements that address security requirements with all of its clients. Where agreements exist, they require ITO and clients to jointly protect assets according to ITO's security framework. However, the security framework is focused on ITO and its data centre and not on what clients need to do. ITO does not provide specific guidance for clients. Therefore, it is not clear what security policies and procedures clients need to follow. Nor does ITO monitor clients to ensure that security policies and procedures currently used by clients are adequate. This has resulted in security weaknesses that could impact all clients. For example, some clients installed software that increased the risk of inappropriate access to systems and data. Until both ITO and clients have strong security processes, client systems and data are at risk.

2. We recommend the Information Technology Office establish information technology security policies for its clients.

Protect client systems and data from unauthorized access

We expect 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. The clients determine who should have access to their systems and data. The client then relies on ITO to make user access changes that it requests. User access controls have become more critical with the increased use of the Internet, online approvals, automated processes, and multiple clients using one data centre.

We expect ITO protects the data centre by configuring, updating, and monitoring its systems against security threats. We also expect ITO secures 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 controls for granting and removing user access when requested by clients. ITO has a process for identifying stale user accounts and reporting these accounts to clients. A user account is stale if 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 implemented processes during the year to help prevent unauthorized persons from accessing the data centre remotely. ITO is also implementing processes for detecting inappropriate or suspicious activity that would affect the data centre. ITO plans to make further improvements

to its monitoring processes to identify attempted security attacks before a breach occurs.

ITO manages over 400 servers, 200 firewalls, and other computer equipment on behalf of clients. ITO uses two firewalls and an intrusion detection system to protect the data centre. The other firewalls protect client locations. To protect client systems and data, ITO needs to configure, monitor, and update the firewalls protecting client locations. However, ITO monitors the client firewalls for availability only. ITO does not have processes to update or monitor client firewalls against security attacks. ITO also needs to consistently update its servers on a timely basis for known security risks.

ITO and its clients need to protect the security of data transmitted between client locations and the data centre. One 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.

We continue to recommend the Information Technology Office protect its systems and data from security threats. We reported this matter in our 2006 Report—Volume 3. The Standing Committee on Public Accounts considered this matter on April 3, 2007 and agreed with the recommendation.

Ensure client systems and data are available for operation

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

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

Even with good backup and recovery procedures, an agency may not be able to continue its operations if a major problem occurred. 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, when cost effective, into systems 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 its systems.

ITO has backup procedures and does backups daily. To help ensure the backups will be available in the event of a disaster, ITO stores the backups offsite.

ITO has developed and approved a disaster recovery plan for its data centre. The plan defines who can activate the plan, identifies staff roles and responsibilities, and includes documentation on systems and recovery processes. ITO has not adequately tested its disaster recovery plan. For example, testing has relied on assumptions, such as equipment being available, that may not be valid in disaster scenarios. ITO needs to do further testing and training to ensure the plan will work as required.

Furthermore, the ITO disaster recovery plan focuses on recovery of the data centre. It does not address client requirements for recovery of their systems and data. Most ITO clients have not yet identified their recovery requirements for key systems and data. Therefore, 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.

We continue to recommend the Information Technology Office have a disaster recovery plan for its data centre and client systems. We reported this matter in our 2006 Report—Volume 3. The Standing Committee on Public Accounts considered this matter on April 3, 2007 and agreed with the recommendation.

Ensure the integrity of the client systems and data

We expect 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. We also expect ITO has strong processes for running and maintaining its data centre.

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 all changes.

Selected references

International Organization for Standardization. (2005). ISO/IEC 27002:2005(E). *Information technology – Code of practice for information security management; 2nd Edition*. Geneva: Author.

Canadian Institute of Chartered Accountants (CICA). (2003). *Trust services principles and criteria*. Toronto: Author.

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

Managing IT service delivery—a follow-up

Background

In 2005, we audited ITO's processes to manage the delivery of agreed-upon information technology services to clients. In Chapter 8 of our 2005 Report – Volume 3, we concluded that ITO had adequate processes to manage the agreed-upon delivery of IT services to clients except for two areas. We found that ITO was delivering IT services without signed service level agreements. We also found that, where there were agreements, they did not include adequate security and disaster recovery requirements.

We recommended that ITO sign service level agreements with its clients prior to delivering information technology services. We also recommended that ITO sign agreements with its clients on security and disaster recovery processes, expectations, and reporting requirements. The Standing Committee on Public Accounts considered these matters in May 2006 and agreed with our recommendations.

In 2006, we followed up on our report by reviewing ITO's actions on our recommendations. We found that ITO and ministry processes had not changed. ITO had continued to provide and ministries continued to obtain services pending negotiation and signing of service level agreements. We also found ITO continued to provide services to clients who had not yet signed security agreements. In addition, the security agreements were not complete. The agreements did not adequately set out security processes, expectations, and reporting requirements for the services provided by ITO to its clients. Nor did the security agreements adequately address disaster recovery processes, expectations, and reporting requirements for services to clients.

In 2008, we again followed up on our report by reviewing ITO's actions on our recommendations. We set out the results of this review in this section.

Signed service level agreements required

We recommended ITO sign service level agreements with its clients prior to delivering information technology services.

Service level agreements set out the roles and responsibilities of both ITO and the client for delivery of IT services. The agreements describe the services to be provided by ITO, service availability requirements (such as the percentage of time networks will be available), service delivery targets (such as establishing new email accounts within five days), and the term of the agreement.

Service level agreements should be in place before ITO provides services to clients so that ITO and its clients understand their respective roles and responsibilities. Without signed service level agreements, there is risk that there may not be appropriate agreement on all matters and that client needs may not be met.

ITO now provides IT services to all government ministries with the exception of Health. ITO has also significantly progressed in signing service level agreements with its clients. At October 20, 2008, ITO had signed service level agreements with all but two ministries that receive IT services. ITO continues to work with these ministries to negotiate service level agreements.

We continue to recommend that ITO sign service level agreements with its clients prior to delivering information technology services.

Security and disaster recovery agreements needed

We recommended that ITO sign agreements with its clients on security and disaster recovery processes, expectations, and reporting requirements.

ITO needs to have agreements with its clients on security and disaster recovery. This is necessary to help ensure the confidentiality, integrity, and availability of systems and data. The agreements could be part of the service level agreements or could be reflected in other documents.

ITO has significantly progressed in signing agreements with clients that specifically relate to security. ITO advises that at October 20, 2008 it had signed security agreements with all but seven ministry clients. In addition, ITO had modified its service level agreements to include additional provisions regarding security. However, ITO's agreements with its clients regarding security do not adequately address reporting on security.

Ministries should request, and ITO should furnish, adequate information regarding security.

The agreements between ITO and its clients regarding disaster recovery have improved. Service level agreements describe general disaster recovery responsibilities and expectations. Ministries have begun to prioritize their recovery requirements, for example, by specifying their most critical applications. However, agreements with ITO still refer to "best effort" for recovery time objective and a maximum seven day recovery point objective (which could put up to a week's data at risk). This is unlikely to meet some clients' needs, particularly for critical applications.

ITO's clients are responsible to require adequate reporting on security and to identify disaster recovery requirements to support their business continuity plans. Until clients clearly identify and communicate their security and disaster recovery requirements, these needs cannot be adequately reflected in the agreements.

We continue to recommend that ITO sign agreements with its clients that address security and disaster recovery processes, expectations, and reporting requirements. We will continue to monitor actions by ITO and ministries in this area.

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.

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.

Recovery point objective—In disaster recovery, the intended point in time before an emergency or disaster to which systems and data can be restored. For example, if backups of data are done every 4 hours, and an emergency or disaster occurs 3 hours after the last backup, then 3 hours of data may not be recoverable. The recovery point objective in this case is 4 hours, and represents the maximum amount of data that management is prepared to lose because of a disaster.

Recovery time objective—In disaster recovery, the point in time after an emergency or disaster by which management plans to have systems and data available. If the recovery time objective for a system is 24 hours, management plans to have that system operational within 24 hours after an emergency.

Service level agreement—An agreement of one agency to provide IT services to another agency. Agreements usually specify the extent and quality of services to be provided.

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.

This page left blank intentionally.