Information Technology Office

6

Main points

The Information Technology Office (ITO) provides information technology (IT) services to client departments. We audited whether the ITO safeguarded public resources and complied with the law. It did so. We also audited the ITO's controls to protect the confidentiality, integrity, and availability of client IT systems and data. As well, we followed up on an earlier service delivery audit.

The ITO has set up the foundation for a secure data centre. During the audit period, the ITO worked at implementing its security processes while it continued to add new clients and provide additional services. We found that the ITO had adequate controls to protect client IT systems and data for the period October 1, 2005 to March 31, 2006 except the ITO needs to:

- perform quality assurance tests to ensure its security policies and procedures are followed
- follow its security policies and procedures
- protect its systems and data from security threats
- implement a disaster recovery plan for its data centre and client systems

To maintain the security of client IT systems and data, the ITO needs to continue to strengthen its processes and monitor its operations as it continues to grow.

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

Introduction

The Information Technology Office Regulations establishes the Information Technology Office (ITO) as a department. The mandate of the ITO includes: "to develop, promote, and implement policies and programs of the Government of Saskatchewan relating to information technology and information management."[1] The ITO carries out this role to support its vision of "enabling excellence in government service delivery through leadership and exceptional customer service in information technology."[2]

For further details regarding the 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 the ITO's major programs and spending. For further detail, see the ITO's 2005-2006 Annual Report available on its website.

	Estimates[3]	Actual[4]
	(in thousands of dollars)	
Central Management and Services	$ 1,407	$ 1,421
IT Coordination and Transformation Initiatives	3,224	3,102
Interdepartmental Services	130	252
Services Provided to External Agencies	69	78
	$ 4,830	$ 4,853

Audit conclusions

The following are our audit conclusions for the fiscal year ending March 31, 2006.

[1] *The Information Technology Office Regulations*, s. 3(b).
[2] Information Technology Office, *Performance Plan 2006-07*, p.5.
[3] *Public Accounts 2005-2006: Estimates*, p.93. The amounts includes Supplementary Estimates of $243,000 (from *2005-06 Supplementary Estimates – November*).
[4] *Public Accounts 2005-2006: Volume 2*, p.135.

In our opinion:

- **the ITO had adequate rules and procedures to safeguard public resources**
- **the ITO complied with authorities governing its activities relating to financial reporting, safeguarding public resources, revenue raising, spending, borrowing, and investing**

The remainder of this chapter discusses the results of our security audit at the ITO and the follow-up of our audit of the ITO's service delivery processes.

ITO security audit

Background

The Information Technology Office (ITO) provides information technology (IT) services to client departments (see Exhibit 2). The ITO's responsibilities include "…operating and managing IT infrastructure (networks and servers), ensuring data security, providing help desk services, developing IT applications, providing project management expertise on all IT projects as well as managing, procuring and distributing IT hardware and software."[5]

Government departments used to provide these services for themselves. By having the ITO deliver these services centrally, the Government intends to reduce costs, increase security, and improve program delivery.[6]

The ITO continues to expand its operations and modify its security processes. The ITO has developed and implemented a security policy based on an international standard. Also, the ITO implemented an IT data centre in May 2005. The data centre stores client data and the hardware and software necessary to run client systems. The ITO uses its data centre to provide IT services to its clients.

[5] Information Technology Office, *Performance Plan 2006-07*, p.4.
[6] Ibid., p.9.

The creation of the new data centre and the addition of new clients are significant changes. For example, when a client joins the ITO, the ITO becomes responsible for hosting and managing client systems. Also, client IT staff become ITO staff. During the audit period, two additional clients joined the ITO. This increased the ITO's staffing levels by over 60%. The ITO needed to train and manage these staff to follow ITO policies and procedures, provide services to new clients on new systems, and continue to serve existing clients.

Our audit objective and criteria

The objective of our audit was to assess whether the ITO had adequate controls to protect the confidentiality, integrity, and availability of client information technology systems and data for the period October 1, 2005 to March 31, 2006.

We used criteria to assess the ITO's processes. The criteria are based upon the *Trusted Services Criteria and Principles* authored by The Canadian Institute of Chartered Accountants, international standards, literature, and reports of other legislative auditors. The ITO agreed with the criteria.

Our criteria, set out in Exhibit 1, describe the key processes that we expected the ITO to use to secure client systems and data.

Exhibit 1

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

1. **Show management commitment to security**
   - 1.1 Responsibility for security is clearly defined
   - 1.2 A threat and risk assessment has been performed
   - 1.3 IT planning supports security
   - 1.4 Management has approved security policies and procedures
   - 1.5 Management monitors security
2. **Protect client systems and data from unauthorized access**
   - 2.1 User access controls protect the client systems from unauthorized access
   - 2.2 Physical security controls protect the data centre from unauthorized access
3. **Ensure client systems and data centre are available for operation**
   - 3.1 System and data backups occur and are tested
   - 3.2 Disaster recovery and business continuity plans are in place
4. **Ensure the integrity of client systems and data**
   - 4.1 Change management processes exist and are followed
   - 4.2 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 the ITO's controls, the confidentiality, integrity, and availability of client systems and data also requires strong security controls at clients. For example, clients need good physical security processes to ensure only authorized users have access to their systems and data. Client security controls were not included in the scope of this audit. However, we are aware of security weaknesses at some clients. For example, not all clients inform the ITO to remove access to staff who are no longer employed. Until both the ITO and its clients have strong security processes, client systems and data are at risk.

Our conclusion

We found that the ITO had adequate controls to protect the confidentiality, integrity, and availability of client information technology systems and data for the period October 1, 2005 to March 31, 2006 except for the matters described in the recommendations below.

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 strong IT division is led by a member of senior management. It is separate from the finance and operating divisions. 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.

The ITO has set up an effective IT organizational structure for securing the ITO data centre. Staff roles and responsibilities are clearly defined and staff meet regularly to discuss IT operation and client issues. The ITO has also set up processes to manage its relationship with clients.

The ITO has developed strong IT security policies and procedures. The ITO is working with clients to have them adopt the ITO's policies and procedures. However, not all clients have defined their security

requirements or signed an agreement to follow the ITO's security policies and procedures. Also, the ITO does not have documented quality assurance processes to ensure that its policies and procedures are being followed.

Without strong quality assurance processes, the ITO cannot ensure that client systems and data are secure and will be available when needed.

1. We recommend the Information Technology Office perform quality assurance tests to ensure its security policies and procedures are followed.

Protect client systems and data from unauthorized access

We expect the ITO to have adequate physical access and user access processes that protect the clients' systems and data from unauthorized access.

Good physical 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, the ITO should physically prevent unauthorized users from entering its data centre.

User access management means protecting information in the IT system from unauthorized access. Access management is more critical with the increased use of the Internet, online approvals, automated processes, and multiple clients using one 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 the ITO to make user access changes that it requests.

The access controls must also establish access rights. Access rights determine what systems, information, and applications a user can see or use. Access rights can also segregate duties within an application.

The ITO has good physical security controls for protecting its IT infrastructure. The data centre is secured with several layers of physical security that are designed to prevent unauthorized access. The ITO has also implemented video surveillance processes for high security areas.

The ITO needs to improve its user access processes as described below.

The ITO needs to follow its security policies and procedures

The ITO has developed strong security policies and procedures based on international standards to protect client systems and data. The policies and procedures identify ITO and client requirements. For example, the client needs to send the ITO an approved access form to support all user access changes including new hires and terminations. The ITO is required to ensure the client change is properly documented and approved before making any changes to a user's access.

The ITO is implementing its security policies and procedures while it continues to obtain new clients, train new staff, and expand its infrastructure. For the period of our audit, the ITO did not consistently follow its established policies and procedures for changing user passwords, making changes to systems, periodically reviewing user access to systems, and for ensuring that user access was promptly removed.

The ITO needs to consistently follow its policies and procedures to protect client systems and data.

2. We recommend the Information Technology Office follow its security policies and procedures.

The ITO needs to protect its systems and data

The ITO needs strong security processes to protect its systems and data.

The ITO has developed strong security controls to protect client systems and data. The security controls are designed to prevent unauthorized access to client systems and data. Also, the ITO has done some testing on the data centre to identify security weaknesses. The ITO identified and fixed security weaknesses that, if exploited, could have allowed

unauthorized access to systems and data. The ITO needs to continue to do ongoing testing to ensure its systems and data are secure.

The ITO needs to implement processes to detect and manage security threats. For example, the ITO needs to monitor security alerts on its network. Without monitoring network alerts, the ITO may not be able to detect security threats quickly.

3. We recommend the Information Technology Office protect its systems and data from security threats.

Ensure client systems and data are available for operation

We expect the 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 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 the ITO and clients. The 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.

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

The ITO does not have a complete and approved disaster recovery plan to restore all systems and data. However, the ITO has drafted a disaster recovery plan for its data centre. The draft plan defines who can activate the plan, identifies staff roles and responsibilities, and includes documentation on systems and recovery processes. The plan does not define recovery time requirements for restoring the data centre. Also, the

ITO needs to make staff aware of their roles and responsibilities, maintain adequate documentation to restore systems, and complete testing to ensure the plan will work as required.

The ITO needs to recover its systems and data before it can start to recover client systems. However, the ITO does not know how long it would take to restore data centre operations. The ITO plans to develop a disaster recovery plan to ensure it can restore systems and data based on client needs. However, most clients have not yet identified their disaster recovery needs. Therefore, neither the 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.

4. We recommend the Information Technology Office have a disaster recovery plan for its data centre and client systems.

Ensure the integrity of the client systems and data

We expect the 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 ensure system changes are approved and tested before implementation. The ITO also needs to ensure that it has strong processes for running and maintaining its data centre.

The ITO has developed strong change management policies and procedures. The ITO has a change management committee that meets weekly to review changes. The ITO also provides integrity by ensuring it has operational processes for managing and maintaining its data centre.

The ITO has adequate processes for making changes to its systems. However, as noted earlier in this chapter, the ITO did not always follow its change management processes.

The ITO has set up the foundation for a secure data centre. To ensure it can maintain the security of client systems and data, the ITO will need to continue to strengthen its processes and monitor its operations as it continues to grow.

Managing IT service delivery—a follow-up

Background

The ITO has been providing IT services to a growing number of clients. Exhibit 2 shows the number of agencies receiving services from the ITO at September 30, 2005 and at September 30, 2006.

In 2005, we audited the 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 reported our audit results.

We concluded that the ITO had adequate processes to manage the agreed-upon delivery of IT services to clients except for two areas. We found that the ITO was delivering IT services without signed service level agreements. We also found that, where there were agreements, they did not include security and disaster recovery requirements.

We recommended that the ITO sign service level agreements with its clients prior to delivering information technology services. We also recommended that the ITO sign agreements with its clients on security and disaster recovery processes, expectations, and reporting requirements.

Exhibit 2—Agencies receiving ITO services[7]

Agencies in IT partnership	At September 30, 2005	At September 30, 2006
	Agriculture and Food	Advanced Education and Employment
	Culture, Youth and Recreation	Agriculture and Food
	First Nations and Métis Relations	Culture, Youth and Recreation
	Government Relations	Executive Council
	Highways and Transportation	Finance
	Industry and Resources	First Nations and Métis Relations
	Northern Affairs	Government Relations
	Rural Development	Highways and Transportation
	Saskatchewan Municipal Board	Industry and Resources
	Saskatchewan Grain Car Corporation	Learning
		Northern Affairs

[7] The ITO also provides services to smaller agencies through agreements with existing partners.

Agencies in IT partnership	At September 30, 2005	At September 30, 2006
		Public Service Commission Regional Economic and Co-operative Development Saskatchewan Municipal Board Saskatchewan Grain Car Corporation
Agencies in the process of joining the IT partnership	Finance Executive Council	Environment
Agencies in discussions with the ITO to join the IT partnership	Community Resources and Employment Corrections and Public Safety Environment Health Justice Labour Learning Public Service Commission Saskatchewan Property Management	Community Resources Corrections and Public Safety Health Justice Labour Saskatchewan Property Management

Source: Information Technology Office

In 2006, we followed up on our report by reviewing the ITO's actions on our recommendations. We set out the results of this review in this chapter.

Signed service level agreements required

We recommended the 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 the ITO and the client for delivery of IT services. The agreements describe the services to be provided by the 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 the ITO provides services to clients so that the 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.

According to the ITO, as of September 30, 2006, the ITO had signed service level agreements with nine of its sixteen clients (agencies in the partnership or in the process of joining). Two service level agreements expired in March 2006 and the ITO is negotiating changes to these agreements. The remaining five departments are also negotiating service level agreements with the ITO.

In our follow-up, we found that ITO and department processes had not changed. The ITO continues to provide and departments continue to obtain services pending negotiation and signing of service level agreements.

The ITO has a standard service level agreement that departments can use as a starting point when joining the partnership. However, most departments obtain services from the ITO before signing an agreement. By doing so, they receive services without adequate assurance that the services, costs, and security they will receive will meet their needs. Departments are subsequently signing agreements as they document their service level expectations.

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

Security and disaster recovery agreements needed

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

The 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.

The ITO has progressed in signing agreements with clients on security. At the time of the audit, the ITO had signed security agreements with two clients. The ITO advises that at September 30, 2006 it has signed security agreements with nine clients. However, the ITO continues to provide services to clients who have not yet signed security agreements.

Moreover, the security agreements are not complete. The security agreements focus on client responsibility to follow the ITO's security policy and standard. The agreements do not adequately set out security processes, expectations, and reporting requirements for the services provided by the ITO to its clients. Nor do the security agreements adequately address disaster recovery processes, expectations, and reporting requirements for services to clients.

However, it is important to note that the clients are responsible to determine their security needs and 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 the ITO sign agreements with its clients that address security and disaster recovery processes, expectations, and reporting requirements.

Further follow-up required

The ITO and its clients should work together to implement agreements that govern service delivery, security, and disaster recovery. The absence of such agreements presents risks to the confidentiality, integrity, and availability of systems and data, and to the ability of the ITO to meet client needs. We will continue to monitor actions by the ITO and departments in this area.

Selected references

International Organization for Standardization. (2005). ISO/IEC 17799:2005(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. (2000). *CoBiT-governance, control and audit for information and related technology; 3rd Edition*. Rolling Meadows, IL: Author.

This page left blank intentionally.