Information Technology Office

14

Main points

The Information Technology Office (ITO) provides information technology (IT) services to client departments. During the year, ITO did not adequately review and approve payroll prior to paying its employees. Also, ITO needs signed service level agreements with its clients prior to delivering information technology services.

As a service provider and custodian of client information systems and data, ITO must have controls to 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:

- 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

Introduction

The Information Technology Office Regulations established the Information Technology Office (ITO) as a department. 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 2006-2007 Annual Report available on its website.

	Estimates[2]	Actual
	(in thousands of dollars)	
Central Management and Services	$ 1,761	$ 1,965
IT Coordination and Transformation Initiatives	4,977	4,814
Major Capital Asset Acquisitions	425	359
Interdepartmental Services[3]	0	(100)
	$ 7,163	$ 7,038

Audit conclusions

The following are our audit conclusions for the fiscal year ending March 31, 2007.

[1] *The Information Technology Office Regulations*, s. 3(b).
[2] *Public Accounts 2006-2007: Estimates*, p.99. The amounts include Supplementary Estimates of $1,468,000 (from *2006-07 Supplementary Estimates – November* and *2006-07 Supplementary Estimates - March*).
[3] ITO provides IT services to client departments on a cost recovery basis. The total billed to client departments for 2006-07 was $42 million.

In our opinion:

- **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. We looked at ITO's controls to protect the confidentiality, integrity, and availability of client IT system and data.

The chapter also provides an update on a recommendation previously made by the Standing Committee on Public Accounts (PAC) that is not yet implemented.

Better control over employees' pay needed

ITO needs to better control employees' pay.

During the year, ITO reviewed its payroll costs during its review of monthly financial reports. However, ITO did not adequately review the accuracy of key payroll data for each pay period prior to paying employees. As a result, employees' pay has not been approved in accordance with *The Financial Administration Act, 1993.*

This weakness increases the risk that employees may be paid incorrect amounts. For example, we noted one instance where an ITO employee was overpaid by about $120,000. ITO recovered this money from the individual.

1. **We recommend that the Information Technology Office adequately review the payroll for accuracy prior to paying its employees to ensure that all employees' pay is approved in accordance with *The Financial Administration Act, 1993*.**

Signed service level agreements required

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. However, most departments obtain services from 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. 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.

As of March 31, 2007, ITO had signed service level agreements with 9 of its 16 clients. The remaining seven departments are negotiating service level agreements with ITO.

We reported this matter in our 2005 Report – Volume 3 and in our 2006 Report – Volume 3. The Standing Committee on Public Accounts (PAC) considered this matter in May 2006 and agreed with our recommendation.

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

ITO security audit

Providing information technology services to clients

ITO delivers information technology (IT) services that government agencies previously managed for themselves. These IT services 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. Through consolidation of information technology services, the Government intends to reduce IT costs, improve the efficiency and effectiveness of IT service delivery, enhance security, use IT to transform internal business processes, and improve citizen/business service delivery.[4]

Responsibility for security

Information technology has become 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 to protect the confidentiality, integrity, and availability of their systems and data.

As a service provider and custodian of client information systems and data, ITO requires adequate processes to protect IT security. 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.

As systems and data are consolidated in one data centre, the potential impact of a security breach increases. Therefore, it is critical that ITO has adequate processes to secure the data centre and data network.

While this audit focused on ITO's controls, the confidentiality, integrity, and availability of client systems and data also require 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. 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 staff who are no longer their employees. Until both ITO and its clients have strong security processes, client systems and data are at risk.

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

[4] Information Technology Office, *Performance Plan 2007-08*, p. 1, 8.

information technology systems and data for the period October 1, 2006 to March 31, 2007.

We used criteria to assess ITO's processes. The criteria are based upon the *Trust Services Criteria and Principles* authored by The Canadian Institute of Chartered Accountants and 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.

Exhibit—Audit Criteria

To ensure ITO has adequate controls to protect the confidentiality, integrity, and availability of client information technology systems and data, 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
   1.6 Management has IT service delivery contracts with clients

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.

Audit conclusion

We found that ITO had adequate controls to protect the confidentiality, integrity, and availability of client information technology systems and data for the period October 1, 2006 to March 31, 2007 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 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 set up an effective IT organizational structure for securing the ITO 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 clients that join ITO. ITO also attends client steering committee meetings.

ITO has implemented adequate IT security policies and procedures. ITO has also performed quality assurance tests. For example, ITO tested physical and user access processes during the audit period. Senior management receives information on quality assurance work performed.

ITO is working with clients to have them implement and monitor security policies and procedures.

Protect client systems and data from unauthorized access

We expect 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, 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 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.

ITO has good physical security controls for protecting its IT infrastructure. ITO has several layers of physical controls that are designed to ensure that unauthorized users do not obtain access to ITO data centre. ITO also has video surveillance processes for monitoring high security areas.

ITO has adequate processes for granting and removing user access as requested by clients. ITO has also implemented a process for identifying stale user accounts starting in January 2007. A user account is stale if not used for over 60 days. The new process identified over 300 stale accounts at clients. ITO is following up with clients to identify what accounts need to be disabled or removed.

ITO has processes for protecting its network. For example, ITO has implemented processes that are designed to prevent unauthorized users from entering its systems remotely. ITO also has processes that can detect inappropriate or suspicious activity inside of its network. We found ITO was not monitoring the above processes to protect its network. As a result, ITO may not identify attempted or successful security breaches.

ITO does not ensure that clients follow its security policies and procedures. This could lead to security weaknesses at a client that would allow an inappropriate user to gain access to the ITO network. While ITO has designed processes to limit inappropriate access, it needs to follow its network monitoring processes. ITO also needs to protect itself from security threats by periodically testing the effectiveness of its security processes and by monitoring the processes followed by clients.

We reported this matter in our 2006 Report – Volume 3. PAC considered this matter in April 2007 and agreed with our recommendations.

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

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

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.

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 backups will be available in the event of a disaster, ITO stores 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 carried out a limited test of the disaster recovery plan just before the end of the audit period. ITO needs to do further testing and training to ensure the plan will work as required.

ITO needs to recover its systems and data before it can start to recover client systems. 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 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 reported this matter in our 2006 Report – Volume 3. PAC considered this matter in April 2007 and agreed with our recommendation.

We continue to 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 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. ITO also needs to ensure that it has strong processes for running and maintaining its data centre.

ITO has adequate change management policies and procedures. These change control processes 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

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.

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 following table provides an update on a recommendation previously made by the Standing Committee on Public Accounts (PAC) that is not yet implemented and is not discussed earlier in this chapter.[5]

PAC REPORT YEAR[6]	OUTSTANDING RECOMMENDATION	STATUS
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 September 30, 2006). A follow-up is planned for 2008-09.

[5] For the definitions of the key terms used in the table, see Chapter 25 – Standing Committee on Public Accounts pages 398 to 399.
[6] PAC Report Year refers to the year that PAC first made the recommendation in its report to the Legislative Assembly.