Information Technology Office

12

Main points **254**

Introduction **255**

Financial overview 255

Audit conclusions and findings **255**

ITO security audit **256**

The importance of IT security 256

Audit objective and criteria 257

Audit conclusion 258

Key findings by criterion 259

Show management commitment to security 259

Protect client systems and data from unauthorized access 260

Ensure client systems and data are available for operation 262

Ensure the integrity of client systems and data 263

Selected references 264

Status of outstanding recommendation of the Standing Committee on Public Accounts **264**

Glossary **266**

Main points

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

Since 2005, we have performed an annual audit of ITO's data centre. Since our first audit, ITO has revised many of its processes and has made modifications to its data centre. However, ITO has not made sufficient progress in addressing security issues.

ITO has adequate controls to protect client IT systems and data except that it needs to:

- provide relevant and timely security reports to its clients
- establish policies that set a minimum IT security standard for clients
- supervise employees to ensure they follow established security policies and procedures
- protect systems and data from security threats
- have a disaster recovery plan for its data centre and client systems

Also, ITO should sign adequate agreements with clients before delivering services to them, have client agreements address security and disaster recovery requirements, and improve its human resource plan.

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 2008-2009 Annual Report available on its website.

	Estimates[2]	Actual
	(in thousands of dollars)	
Central Management and Services	$ 1,958	$ 1,957
IT Coordination and Transformation Initiatives	3,367	3,365
Major Capital Asset Acquisitions	250	161
Inter-ministerial Services	---	(19)
	$ 5,575	$ 5,464

ITO provides IT services to clients on a cost recovery basis. The total billed to clients in 2008-09 for these services was approximately $62.9 million.

Audit conclusions and findings

In our opinion for the year ended March 31, 2009:

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

[1] *The Information Technology Office Regulations, 2007*, s. 3(b).
[2] Saskatchewan Finance, *2008-2009 Saskatchewan Estimates*.

- **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 provide an update on recommendations previously made by PAC that are not yet implemented.

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."[3]

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

ITO states that it provides IT services to 24 government ministries and agencies (clients), including more than 12,000 government employees.[4]

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.

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 security risks are managed at client locations and whether clients are meeting their security

[3] The Information Technology Office Regulations, s. 3(c).
[4] www.ito.gov.sk.ca/consolidation (Oct 16, 2009).
[5] ITO has one main data centre and additional data centres that it uses for testing and backup purposes.

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 September 1, 2008 to February 28, 2009.

While this audit focused on ITO's controls, adequate security requires that both ITO and clients have strong security controls. 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.

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, 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 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.

Audit conclusion

Since 2005, we have performed an annual audit of the data centre. Since our first audit, ITO has revised many of its processes and has made modifications to its data centre. However, ITO has not made sufficient progress in addressing security issues. As we describe later in this chapter, weaknesses we have identified in prior years continue to exist. ITO needs to address its security weaknesses.

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 September 1, 2008 to February 28, 2009, except it needs to:

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

In the sections below, we describe our expectations (in italics) and key findings.

Key findings 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. 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 has set up processes for integrating new clients. ITO meets regularly with its clients.

ITO has defined key goals and objectives related to security in its strategic plan. 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. Senior management receives information on quality assurance results. The assurance work performed by ITO confirms that security weaknesses exist.

Clients receive limited information on ITO weaknesses. ITO does not provide our audit report on security to clients nor does it explain the potential impact of its weaknesses on client systems and data. ITO could not tell clients when its security issues would be resolved.

1. We recommend the Information Technology Office provide relevant and timely security reports to its clients.

At February 2009, ITO has agreements with most, but not all, of its clients. The agreements 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 to clients on what security policies and procedures clients need to follow. Nor does ITO assess the adequacy of security policies and procedures currently used by clients. 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, systems and data are at risk.

We continue to recommend the Information Technology Office establish information technology security policies for its clients. Security policies would set a minimum standard clients must follow. If a client does not meet the minimum standard, all client systems and data managed by ITO could be at risk. We reported this matter in our 2008 Report – Volume 3. PAC considered this matter on December 10, 2008 and 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. 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). However, ITO employees did not consistently follow policies and procedures for removing user access. For example, former ITO and client employees continued to have access to systems and data during the audit period.

ITO has adequate policies and procedures for changing passwords and periodically reviewing access to systems and data. ITO evaluated its processes and found that its employees were not following the policies and procedures. ITO needs to ensure employees consistently follow procedures for responding to client requests. For example, employees did not consistently verify the identity of users who request password changes.

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, ITO did not install all important updates (i.e., patches) for servers during the audit period. Management was aware that not all updates were installed.

2. We recommend the Information Technology Office supervise its employees to ensure they follow established security policies and procedures.

ITO and its clients must 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.[6] 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.

ITO manages over 400 servers, 200 firewalls, and other computer equipment. ITO has two firewalls and an intrusion detection system at the data centre. In addition, ITO has firewalls at client locations. ITO monitors the intrusion detection system. This helps ITO detect inappropriate activity on its network on a timely basis. However, ITO does not monitor firewalls for security attacks. Also, ITO does not update firewalls at client locations.

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

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

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 but needs to improve its monitoring to ensure all data is successfully backed up. ITO stores data backups off-site to help prevent data loss if the data centre is destroyed. ITO did not consistently transfer its backup data off-site on a daily basis.

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.

The ITO 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 has never fully tested 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 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. PAC considered this matter on April 3, 2007 and 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 all 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 (CICA). (2003). *Trust services principles and criteria*. Toronto: Author.

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

IT Governance Institute. (2006). IT Control Objectives for Sarbanes-Oxley: *The role of IT in the design and implementation of internal control over financial reporting, 2nd Edition*. Rolling Meadows, IL: Author.

The Information Systems Audit and Control Foundation. (2005). *CoBiT4.0*. Rolling Meadows, IL: Author.

Status of outstanding recommendation of the Standing Committee on Public Accounts

The following table provides an update on recommendations previously made by PAC that are not yet implemented and are not discussed earlier in this chapter.[7]

[7] For the definitions of the key terms used in the table, see Chapter 20 – Standing Committee on Public Accounts.

PAC REPORT YEAR[8]	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, 2009). ITO has not signed service level agreements with four of its clients.
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, 2009). ITO is in the process of drafting a new agreement template.
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, 2009). ITO is in the process of developing a new human resource plan for 2010-11.

[8] 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.

This page left blank intentionally.