Processes needed to manage IT

7

Main points **200**

Introduction **201**

Key IT risks faced by the Government **201**

Key IT management processes **202**

IT planning and supervision 202

Key IT planning and supervision processes 202

Change management practices 203

Key change management processes 204

IT operations and support 205

Key IT operations processes 206

Security 207

Key security processes 207

Security and privacy management 207

User access controls 208

Physical access and environmental controls 208

IT contingency planning 209

Key contingency planning processes 209

What is next? **209**

Exhibit 1 – Audit criteria for IT Management **210**

Selected references **211**

Main points

Information and related information technology (IT) plays a critical role in the delivery of important government services The Government has also spent considerable resources updating and replacing IT systems in the last five years. Currently the Government is replacing the payroll and human resource systems used by departments. The Government is also consolidating some of its IT infrastructure and IT management. These new and planned IT changes are large, complex, and risky. The Government must manage these new risks well.

In this chapter, we outline key IT management processes we will use as criteria when auditing Government's management of IT systems. IT management includes IT planning and supervision, change management, operations and support, security processes and contingency planning. It is important that Government, its agencies, and its supervisory agencies use best practices to ensure the security, integrity, availability and confidentiality of IT information and its related systems.

Introduction

Information and related information technology (IT) plays a critical role in the delivery of important government services. The results of our 2002 security survey[1] showed the Government as a whole planned to spend over $300 million on IT in 2003. IT includes computers, networks, applications, data, and IT staff support. Governments face significant risk in managing a complex resource like IT. To achieve its objectives, the Government must have good information technology management processes.

In this chapter, we identify good IT management processes based on current standards. We will audit government agencies using these processes as criteria. We will also assess the role of the Government, its agencies, and supervising agencies in ensuring they use good IT management processes.

Key IT risks faced by the Government

The Government has a large and complex IT environment that faces significant risks. If the Government and its agencies and supervising agencies cannot manage their IT risks, they may not be able to deliver their services and achieve their objectives.

Key IT risks include:

- unauthorized access to IT information or infrastructure;
- IT systems are not available when needed;
- IT planning and decisions do not achieve agency objectives;
- IT information is incomplete, inaccurate, late, or unauthorized;
- personal information is used inappropriately;
- IT systems are late, over budget, or do not achieve intended benefits or objectives;
- information is disclosed inappropriately; and
- ineffective use of public IT resources.

[1] 2002 Fall Report Volume 2 – Chapter 3

Key IT management processes

The Government needs to follow good IT management processes to manage its risks and achieve its objectives.

In this chapter, we describe processes consistent with current standards including those developed by the Information Systems Audit and Control Foundation (ISACA), IT Governance Institute, The Canadian Institute of Chartered Accountants (CICA), and the Project Management Institute (PMI). We list some standards by these and other agencies in the selected references at the end of the chapter. We summarize these processes under the following categories:

1. IT planning and supervision;
2. change management practices;
3. IT operations and support;
4. security; and
5. IT contingency planning.

In this chapter, we outline why the Government must manage these processes well. We will also identify key processes under each category.

IT planning and supervision

The Government, its agencies, and supervising agencies need to ensure they have the planning and supervision processes needed to ensure good IT management. A strong organizational structure ensures accountability and supervision of IT systems. For example, the Government has delegated responsibility for supervising the security of CommunityNet to the Information Technology Office (ITO). It is important that the ITO has the authority and is accountable to manage security.

Key IT planning and supervision processes

Key IT planning and supervision processes include:

- an IT organizational structure that ensures accountability for IT;
- IT planning that supports the agency's goals and objectives;
- an IT risk assessment processes; and

- processes to ensure compliance with authorities and other external requirements.

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 IT meets the agency's needs. Finally, it ensures its employees are competent and adequately trained.

Good IT planning ensures:

- IT meets the agency's objectives;
- IT systems are based on a strong IT architecture; and
- the maintenance of a strong IT infrastructure.

The plan for the agency should have performance targets linked to organizational strategies and objectives for both operations and projects. The plan should also set out how the overall design of the components of the IT systems fit and work together for the agency and the Government as a whole. This is the IT architecture.

The IT infrastructure is a key component that includes the computers, networks, and software needed to run the business applications. The key to management of infrastructure is planning, accountability, capacity, and reporting its targets and results.

IT policies should cover security, contingency planning, and information management and be based on a threat and risk assessment. The policies must reduce the threats to an acceptable level that allows the agency to meet its objectives. The agencies must monitor compliance with policies. The agencies must also ensure its policies comply with its authorities.

Change management practices

The Government needs to ensure that new IT systems and changes to its IT systems meet its objectives. There have been significant changes to the IT environment in Saskatchewan in the past few years. In previous chapters, we have reported on the ITO's CommunityNet, Finance's MIDAS project, SaskPower's Delta project, SaskEnergy's One World, and Information Service Corporation's Land System. These projects have cost over $200 million and have changed the IT risks facing the Government.

It has increased the dependency on the Internet and large agency-wide systems. The well-publicized Internet risks require careful management. In the agency-wide systems, the Government has used public resources to implement four different systems in the last five years.

Following strong processes will help to ensure that the Government develops or implements secure IT systems that achieve benefits on time and on budget. It is important that agencies implement systems based on the Government's vision and architecture. It is easier to develop or purchase a system in isolation, because it is generally less expensive and requires no coordination with other agencies. However, it may not meet similar needs of other government agencies. In Chapter 6 of our 2003 Report – Volume 1 on developing a system to share water quality information we highlight the need to develop systems based on the needs of a group of government agencies.

Key change management processes

Key change management processes include:

- system development processes;
- approved policies and procedures to acquire and dispose of IT systems; and
- processes over changes to its IT systems.

Ensuring government agencies properly purchase or develop a new system requires key processes including a business case, project management, and a system development life cycle.

A business case ensures that all systems are approved knowing the project scope, full cost, and the future benefits. The business case should also ensure the new system fits in the Government's architecture.

Government agencies should use project management processes including the nine management processes set out in the Project Managements Institute's *Project Management Body of Knowledge* (PMBOK). The standard sets out processes to help ensure projects are on time, on budget, and achieve benefits. This includes compliance with contracts and other authorities including the purchase and disposal of IT

assets. The standard also covers human resource management, communication, and quality assurance.

Finally, a system development life cycle is a process to take the vision in the business case and implement it as an IT system that achieves the planned benefits. There are many models in use today. The types of life cycles available are set out in the PMBOK and other sources.

Government agencies must acquire and dispose of IT systems using approved policies and procedures.

The need to change systems properly is a goal of all agencies. The steps to change an IT system include a documented and approved request, multiple levels of testing, final approval, and a process to move the change to the live system. There should also be a quality assurance review after the change is complete. The quality assurance process ensures adherence to standards and the meeting of requirements.

IT operations and support

Government agencies must ensure their IT systems operate well. If not, data may lack integrity, performance may be slow, or systems may not be available when needed. All government agencies connect to the Internet and many use CommunityNet. They must take extra precautions due to threats from outside their networks. Government agencies must also manage internal threats because a loss, mistake, or inappropriate use by an employee may be costly.

The Government must protect their operations carried out by outside service providers (OSP) with service level agreements and audits. Government agencies may contract with an OSP to do some of its critical IT operations. For example, the ITO is now managing some departments' infrastructure. To do this the ITO must establish agreements with the departments that set out levels of service expected and how it is accountable for this service.

Currently in the Government, most audits of OSP operations assess and report the existence of controls on a date. It is important that auditors assess and report the effectiveness of the OSP controls over the whole year.

Key IT operations processes

Key IT operations processes include:

- protecting the applications, ensuring data integrity, and meeting the users' control needs;
- backup and recovery procedures;
- monitoring and reacting to incidents; and
- monitoring outside service providers affecting IT operations or support.

IT operations include balancing important processes, monitoring of system performance, and reacting to problems that may affect integrity of data or delay the completion of processes. Operations must ensure the security and integrity of IT systems. Government agencies use a service level agreement to set out expectations if an OSP carries out the operations. Operations also include user support and help desk functions to answer questions and fix problems. Standards for quality include the IT Service Management Forum's *IT Infrastructure Library* (ITIL).

IT operations also include good backup and recovery processes. Even with good operating procedures, files may be lost and processes may fail. Good backup and recovery aids in meeting user expectations for availability.

IT operations must monitor and react to incidents and security breaches. A help desk function often carries out this process. Operations must also be proactive to fix known risks by quickly updating systems.

If government agencies contract out their data centre or help desk, it is critical that they have a service level agreement, even when it is with another government agency. The agreement should include performance expectations, security requirements, penalties for non-performance, and the ability to audit.

The Canadian Institute of Chartered Accountants (CICA) has standards for these audits called *5900 - Opinions on Control Procedures at a Service Organization.* The CICA also has criteria for this audit set out in *Trust Services Principles and Criteria.*

Security

The Government must ensure it has effective security controls over its IT systems including data and infrastructure. The Government also needs to classify information based on the need for security, confidentiality, integrity and availability. The ITO is asking Government departments to use an information classification standard. However, the ITO lacks the authority to enforce its use. Without good policies and access controls, people may use confidential and private information inappropriately. Poor security can affect the integrity and availability of IT systems.

Key security processes

Key security processes include security and privacy management, user access controls, and physical and environmental controls. The following describe each of these components.

Security and privacy management

It is important that government agencies base their policies for security and privacy management on a threat and risk analysis and a government-wide policy. The Government, its agencies, and its designated supervisory agency must monitor compliance with the policy. The policy should cover not only security but also governance, operations, and change management. An example of a recognized standard for a policy that covers most of these areas is ISO/IEC 17799[2]. There are also standards used by the Government of Canada and the United States Government. A recognized standard for privacy is the Canadian Standards Association's *Model Code for the Protection of Personal Information*. There is also provincial legislation governing privacy.

Each agency should do a threat and risk analysis using a recognized standard. The RCMP's *Threat and Risk Assessment for Information Technology* and the Australia and New Zealand standards Associations' *AS/NZS 4360*[3] are both good standards for a risk assessment. The Government and its agencies need to do a risk assessment to ensure they have reduced their risks to an acceptable level.

[2] International standards Organization: Information Technology – *Code of practice for information security management.*
[3] AS/NZS 4360:2004 : *Risk management*

User access controls

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, CommunityNet, on-line approvals, and automated processes.

User access controls reduce the risk of unauthorized access. 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 verifies who the user is and grants access. It is also critical that government agencies can verify any person or process that connects to its IT systems.

The access controls must also establish rights. Access rights control what systems, information, and applications a user can see or use. Access rights can also segregate duties within an application. When contractors need to use government systems, they should follow the agencies standards and be closely monitored. Finally, all access should be for a limited time and be reviewed periodically.

Physical access and environmental controls

Good physical and environmental controls means protecting IT infrastructure from harm. Physical access controls protect all computers, network devices, disk drives, backup devices, and wiring from unauthorized access. Good security management means an agency protects its IT assets from environmental threats like fire, flood, heat, or dust.

Protecting IT system assets from damage from hazards is complicated because assets are in multiple locations, use wireless links, and are often in the care of an outside service provider. Good processes for physical and environmental controls include ITIL and the manufacturers' recommendations.

IT contingency planning

The Government, its agencies, and supervising agencies should have strong plans to recover systems in the event of a disaster like a fire or flood. It is also important agencies plan for the total recovery of all key business processes in the event of a disaster. 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. Contingency planning is broken into two components. The first is disaster recovery or processes to recover and return an IT infrastructure to operations after a disaster. The second is business continuity planning which is a process to return business processes to operation after a disaster.

Key contingency planning processes

A contingency planning process should:

- set out the responsibilities to implement the plan;
- establish emergency procedures to be used while the system is unavailable;
- include steps for the recovery and restoration of the system or business process;
- document the key system or business processes, and procedures; and
- be regularly tested and updated.

What is next?

Exhibit 1 shows the key processes we will use as criteria to assess the management of IT in government agencies with significant IT systems. As risks change and standards evolve, these criteria will continue to develop. It is important that Government, its agencies, and its supervisory agencies use best practices to manage IT. Using best practices will help to ensure the security, integrity, availability and confidentiality of IT information and its related systems.

Exhibit 1 – Audit criteria for IT Management

There are adequate processes to:

1.0 Plan and supervise IT systems.
- 1.1 Management has established an IT organizational structure that is conducive to adequate controls and preparation of adequate financial statements.
- 1.2 Management is committed to ensuring IT supports the agency's goals and objectives.
- 1.3 Management has adequate IT risk assessment processes.
- 1.4 Management has adequate processes to comply with authorities and other external requirements.

2.0 Develop, acquire, or change IT systems.
- 2.1 Management has adequate system development processes.
- 2.2 Management has adequate approved policies and procedures to acquire and dispose of IT systems.
- 2.3 Management has adequate change management processes over changes to its IT systems.

3.0 Operate and support IT systems.
- 3.1 The agency has adequate IT operations and support processes to protect the production environment and meet the users control needs.
- 3.2 The agency has adequate backup and recovery procedures.
- 3.3 The agency has adequate processes to monitor and react to incidents.
- 3.4 The agency has processes to monitor third party service bureaus or other outsourcing agreements affecting IT operations or support.

4.0 Manage security.
- 4.1 The agency has adequate security and privacy management.
- 4.2 There are adequate user access controls.
- 4.3 There are adequate physical and environmental controls over IT facilities.

5.0 Test and approve business or disaster contingency plans.

Selected references

International Organization for Standardization. (2000). *Information technology: code of practice for information security management.* Geneva, Switzerland: ISO. (Reference number ISO/IEC 17799: 2000).

Project Management Institute. PMI Standards Committee. (1996). *A guide to the project management body of knowledge - pmbok guide*. Upper Darby, Pennsylvania: Author.

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

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

The Canadian Standards Association. (1996). *Model code for the protection of personal information*: Toronto Author.

The IT Services Management Forum. (2001*). IT Infrastructure Library - ITIL service delivery*, Earley, Reading, UK: Author.

The Information Systems Audit and Control Foundation. (2000). *CoBiT-governance, control and audit for information and related Technology*. Rolling Meadows, IL: Author.

The Information Technology Office. (2003). *Annual Report 2003-2004*. Regina: Author.

Thorp, J. and DMR's Centre for Strategic Leadership. (1998). *The information paradox*. Toronto, Canada: McGraw-Hill Ryerson Limited.

This page left blank intentionally.