Service Alberta
Information Technology Disaster Recovery Program Followup

Auditor General
OF ALBERTA

Report of the Auditor General
November 2019

Contents

Related Reports:

- Service Alberta: IT Disaster Recovery Program (October 2014)
- Service Alberta: Protecting Information Assets Followup (October 2012)
- Alberta Health Services: Develop a Detailed Plan for Implementing Risk-based Disaster Recovery Processes (October 2015, p.103)
- Service Alberta: Systems to Manage a Comprehensive Inventory of IT Applications (May 2017)
- Alberta Health Services: Information Technology Control Policies and Processes (November 2018, p.86)
- Athabasca University: Information Technology Resumption Plan (November 2018, p.17)

Appointed under *Alberta's Auditor General Act*, the Auditor General is the legislated auditor of every provincial ministry, department, public post-secondary institution, and most provincial agencies, boards, commissions, and regulated funds. The audits conducted by the Office of the Auditor General report on how government is managing its responsibilities and the province's resources. Through our audit reports, we provide independent assurance to the 87 Members of the Legislative Assembly of Alberta, and the people of Alberta, that public money is spent properly and provides value.

Report Highlights

An IT application is a single or group of programs used to do certain tasks. Common IT applications are email, internet browsers, and database software p. 3

Some critical Government of Alberta IT applications include:

- Alberta Netcare Portal
- motor vehicle registry
- information or evacuation payments in disasters and emergencies
- payments for equipment and supplies for people with long-term disabilities or chronic illness

p. 3

Albertans require that IT applications and systems that provide critical government services be restored as soon as possible after a disaster p. 2

We have repeated our 2014 recommendation to Service Alberta p. 6

Without proper IT disaster recovery capabilities, the government may not be able to deliver essential services when disasters occur p. 5

At the time of our audit, there were over 200 applications yet to be assessed for criticality. For 194 other applications assessed as critical, we found:

- over one-quarter had no documented disaster recovery plan
- less than one-quarter were tested for recovery in 2018
- nine failed their last recovery test

p. 7

Our audit objective was to determine if Service Alberta implemented our 2014 recommendation to ensure critical Government of Alberta IT applications were identified, tested, and recovered within required timelines p. 4

Service Alberta has made process improvements since 2014, and progress has been made in assessing criticality of applications. Of the 1,500 applications in use across government, departments have determined the criticality of 1,300 p. 7

Summary

Almost everyone has experienced their phone or computer crashing and the frustration of not knowing when or if the device can be fixed. When IT systems or services go down, we quickly find out which ones severely impact our daily lives and need to be restored.

Albertans require that IT applications and systems that provide critical government services be restored as soon as possible after a disaster.

When we first audited the government's IT disaster recovery capabilities in 2014, we found it lacked processes to identify the most critical applications to Albertans and to ensure they were available when needed. We recommended that Service Alberta improve processes to identify critical applications across government departments and ensure they are adequately tested for recovery.[1]

In this followup, we found Service Alberta has made a number of process improvements since 2014, including:

- developing a framework that provides IT disaster-recovery requirements, tools, and guidance to departments
- developing a central repository to track disaster-recovery-related information for all IT applications across government
- developing recovery time requirements for IT applications based on criticality categories
- implementing an annual exercise to help departments test the recovery of critical IT applications

We also found that Service Alberta has more work to do.

While the criticality assessments of 1,300 IT applications have been completed, more than 200 applications have yet to be assessed. Service Alberta does not ensure that all IT applications assessed as critical by departments comply with its IT disaster recovery policies, and it does not follow up with departments when IT disaster recovery requirements are not met.

Until these process weaknesses are fixed, Service Alberta cannot assure Albertans that all critical services they rely on can be promptly recovered if they go offline.

As a result, we repeat our 2014 recommendation.

[1] As government ministries managed their own IT systems at the time of our original audit, our original recommendation noted Service Alberta needed to work with the government's Deputy Minister's Council to implement our recommendation. Service Alberta has since been assigned single oversight responsibility on IT disaster recovery over government ministries, excluding agencies, boards, and commissions.

Background

An IT application is a single or group of programs used to do certain tasks. Common IT applications are email, internet browsers, and database software. The Government of Alberta relies on IT applications to provide essential services to Albertans. We expect that government departments have processes to identify and maintain IT applications that support essential services provided to Albertans. These applications should be considered critical by departments.

Every day, Albertans rely on a wide range of government programs and services that depend on IT systems and applications. Albertans need to know that if unexpected outages occur, government can quickly restore these programs and services.

Healthcare facilities provide services such as routine doctor visits, medical diagnostics, and emergency medical treatment. These facilities rely on IT applications, such as Netcare or the Pharmaceutical Information Network, to provide vital health data and patient medication histories.

According to the open government portal, there are over three million licensed drivers in Alberta. Service Alberta's Motor Vehicles System records licenses and registration information for these drivers.

The Department of Municipal Affairs uses IT applications to manage emergency and disaster preparedness, prevention, response, and financial assistance. Applications such as the AEA (Alberta Emergency Alert) and AEA Mobile (Alberta Emergency Alert Mobile) alert Albertans when a disaster or emergency event occurs.

People with disabilities or chronic or terminal illnesses rely on Alberta Aids for Daily Living for financial assistance and support for equipment and supplies. This support is critical to allow these Albertans to maintain their independence at home or in care.

About this Audit

In 2012, a fire in the Shaw Court building in Calgary left its data centre unusable. As a result, many public and private organizations could not carry on normal operations. Government entities had disaster recovery plans, but actual recovery times were delayed up to one week. So were programs and services. This fire prompted our 2014 audit of the government's IT disaster recovery program. We found that government lacked effective processes to identify its most critical IT applications and to ensure they were available to Albertans when needed, and we recommended improvement.

Objective and Scope

Our objective was to determine if Service Alberta has implemented our 2014 recommendation to:

- identify the most critical IT applications throughout all government departments
- identify the timelines, after a disaster, that critical IT applications must be recovered
- ensure that there are tested plans and adequate resources to recover critical IT applications within those timelines

We audited the department's IT disaster recovery processes and oversight in place from our 2014 recommendation to April 2019. We did not include agencies, boards, and commissions (ABCs) in the scope of our audit. Since 2014, Service Alberta has clarified it is responsible for IT disaster recovery of critical government department IT applications. Service Alberta has indicated it is not responsible for agencies, boards, and commissions. ABCs are responsible for recovering their critical IT infrastructure and applications.

Criteria

We used criteria from our original audit to assess if Service Alberta has implemented our recommendation. Service Alberta management acknowledged the suitability of the audit criteria on August 10, 2018.

What We Examined

To assess implementation, we:

- examined Service Alberta's processes to identify IT applications across government and assess their criticality
- examined processes to define the target recovery timelines for IT applications and to ensure plans and resources exist to recover applications within targeted timelines
- interviewed department management and staff responsible for these functions
- analyzed the application catalogue and reviewed disaster recovery planning and testing documentation

We conducted our fieldwork between September 2018 and April 2019 and completed our audit on September 12, 2019.

Conclusion

We conclude that Service Alberta has not implemented our 2014 recommendation to ensure critical IT applications are identified, tested, and recovered within required timelines. Audit criteria not met were oversight of business impact assessments, defined recovery timelines for all applications, adequacy of disaster recovery plans, and testing of those applications.

Why This Conclusion Matters to Albertans

IT systems are crucial to delivering government programs and services to Albertans. Without proper IT disaster recovery capabilities, government may not be able to deliver essential services when disasters occur. Albertans expect that if critical government IT applications—including key systems for health and safety—are disrupted, government can and will recover them in a timely manner.

Summary of Recommendations

REPEATED RECOMMENDATION:
Improve recovery of critical information technology applications

We again recommend that the Department of Service Alberta:

- identify the most critical IT applications throughout all government departments
- identify the timelines, after a disaster, that critical IT applications must be recovered
- ensure that there are tested plans and adequate resources to recover critical IT applications within those timelines

Detailed Findings and Recommendations

Improve Recovery of Critical IT Applications

REPEATED

Context

Service Alberta provides core IT infrastructure[2] services, such as network connections, security, and email to government. Service Alberta is also responsible for the recovery of core government IT services and business resumption. Service Alberta provides oversight to ensure critical IT infrastructure, including IT applications, is identified and recoverable within required timelines. Individual government departments own applications hosted on the IT infrastructure.

Successful recovery of IT applications requires Service Alberta and departments to work together to prepare for major service disruptions before they happen. Departments are responsible for assessing the criticality of their own applications, developing disaster recovery plans, and working with Service Alberta to test recovery of their applications. Service Alberta is responsible for oversight of these activities, which involves setting disaster recovery guidelines and requirements, monitoring the work to ensure requirements are met, and following up on any gaps or deficiencies.

Service Alberta is currently centralizing most department-managed IT resources to allow for more effective oversight of IT assets. Under this transformation project, Service Alberta will manage IT assets in departments. By leveraging resources across departments, Service Alberta will be able to prioritize and work with departments to test disaster recovery of critical IT infrastructure and applications.

To recover from a disaster or significant disruption in service delivery, the data centre environment (for example, electrical power, air cooling, and network connectivity to other locations) must be operational and safe before returning the IT infrastructure to service. IT applications can be reinstalled or restored to operation once the three essential layers of disaster recovery—people, data centres, and hardware—are available and operational.

There are many different groups involved in disaster recovery efforts—data centre owners, IT groups, application owners, and users. Effective and clear communication and knowledge of disaster recovery plans is essential to returning services to normal as soon as possible.

Our 2014 audit found that a government-wide process or comprehensive plan to identify the most critical applications to the government and Albertans and to ensure they are available when needed did not exist. There was no assurance that recovery of IT applications could be on time, and departments lacked formal processes to test disaster recovery capabilities for their applications. We recommended Service Alberta improve those processes.

Criteria

The department should have effective processes to:

- perform or obtain business impact or risk assessments for IT applications from all departments
- define the targeted recovery timelines needed for each IT application based on need, risk, and cost
- ensure adequate plans and resources exist to recover IT applications within the targeted timelines

[2] Computers hosting IT applications or data and the networks that link them together.

Our followup audit findings

Key Findings

- Service Alberta has made process improvements and progress in oversight of criticality assessments of IT applications across government departments. But these assessments are not complete—over 200 applications have not yet been assessed for criticality.
- Service Alberta does not ensure compliance with its IT disaster recovery policies. Departments assessed 194 applications as critical. Of these:
  - over one-quarter have no documented disaster recovery plan
  - less than one-quarter were tested for recovery in 2018
  - nine failed their last recovery test
- Service Alberta does not follow up with departments on deficiencies related to criticality assessments, disaster recovery plans, and testing of IT applications.

Identifying critical IT applications and defining their targeted recovery timelines

Since 2014, Service Alberta developed an IT disaster recovery framework with policies, standards, guidance, and tools to help departments with recovery solutions. Departments are responsible for assessing the criticality of their own applications. To assist with this process, Service Alberta developed a Business Impact Assessment (BIA) tool to help departments identify recovery requirements for their applications and understand the impact of a disruption in their systems. If all departments use the tool, then it should provide a consistent criticality assessment. Service Alberta has not mandated that departments use the BIA tool and does not collect completed assessments. As a result, departments are at increased risk of inconsistently assessing criticality of their applications or not assessing criticality at all.

Criticality is the main factor in determining the Recovery Time Objective (RTO)[3], the maximum time an application or system can be out of service. Service Alberta developed the RTO categories in the figure below to help departments identify applications ranging from business critical to non-critical and give them better clarity on recovery expectations.

In 2017, Service Alberta implemented an *Application Catalogue* to identify and track IT applications across government. Departments should record key information in the catalogue, such as application criticality, the availability of disaster recovery plans, and dates and results of recovery tests. If used effectively, the catalogue is a good first step for Service Alberta to identify and track the status of IT applications across government. It can be used to determine if departments have assessed their applications for criticality and if disaster recovery requirements are being met for critical applications.

As of January 2019, the application catalogue listed over 1,500 active IT applications across government departments, all of which should be assessed and assigned a criticality rating. At the time of our audit, departments have made progress, having assessed 1,300 of these applications for criticality, but more than 200 applications have yet to be assessed. The problem is more prevalent in some departments than others. For example, the Department of Environment & Parks has not assigned criticality ratings to 80 of its 160+ applications. The Department of Justice & Solicitor General has not assigned criticality ratings to 40 of its 80 applications, and the Department of Advanced Education has not assigned criticality ratings to one-third of its 180 applications.

Service Alberta's disaster recovery policy delegates responsibility to departments to assess and document the criticality of their applications using the IT disaster recovery framework. But as part of its oversight responsibility, we expect Service Alberta to use the catalogue to ensure criticality assessments are done for all IT applications and follow up with departments where gaps exist. This oversight process may include requesting supporting documentation, verifying information in the catalogue, and developing action plans based on anomalies identified. Service Alberta provided no evidence of this followup with any of the departments that have not assigned criticality ratings to all of their IT applications.

[3] The targeted timeline defined by the business or process owner during which an IT system must be restored after a disaster.

Recovering IT applications within targeted recovery timelines

As of January 2019, the catalogue shows 194 of the 1,300 applications assessed by departments are "critical." Service Alberta's policy mandates that departments must develop, implement, maintain, and test IT disaster recovery plans for all their critical IT applications. We found, however, in our examination of the catalogue that departments are not complying with this policy, as over one-quarter of the 194 critical applications do not have disaster recovery plans.

Service Alberta delegated responsibility to departments for assessing criticality of their own IT applications and ensuring critical applications are tested for recovery. Service Alberta should be using the catalogue to identify any critical applications across government that do not have documented disaster recovery plans and follow up with departments accordingly. Instead, Service Alberta stated to us that it assumes applications without disaster recovery plans are not critical. It provided no evidence that it followed up with departments to verify the criticality of applications without plans or that it worked with those departments to ensure they developed and tested plans.

Some departments appear to be doing a better job than others at documenting disaster recovery plans. Eight departments indicate in the catalogue that disaster recovery plans are in place for all of their critical applications. But two departments—Environment & Parks and Community & Social Services—indicate documented disaster recovery plans exist for only two of their combined 36 critical applications. Critical information systems related to flooding, water and fire data, and timber production management at Environment & Parks and dental, drug, and other payment processing at Community & Social Services are at higher risk of not being available if disaster recovery plans for those systems are not developed and tested regularly.

Service Alberta policy states that information and IT systems must be backed up and the recovery process tested regularly. Service Alberta stated to us that it assumes that applications are not critical if departments have neither tested them within the previous 12 months nor scheduled them to be tested in the next 12 months. We found the catalogue tracks when department applications were last tested, but it does not indicate the next scheduled testing date. As a result, Service Alberta cannot rely solely on the catalogue to conclude whether departments test critical applications as required.

In 2016, Service Alberta began an annual disaster recovery exercise to test the recovery of core IT infrastructure to an alternate data centre. Departments must conduct recovery tests for their own applications, and they can choose to do this during Service Alberta's annual exercise.

In the 2018 annual disaster recovery exercise, 21 departments participated and tested almost 300 applications. The application catalogue indicated, however, that less than one-quarter of the 194 applications assessed as critical were tested in 2018, including during the annual exercise. We found in our examination of the catalogue departments are not complying with requirements to regularly test recovery of their critical applications. Because the catalogue does not show the next scheduled testing date, we expect Service Alberta to follow up with departments having critical applications that, according to the catalogue, were not tested in 2018. We found no evidence that Service Alberta followed up with departments to ensure the catalogue is accurate and complete and to determine the next scheduled testing dates for critical applications not tested in 2018.

Only two departments recorded in the catalogue that all critical applications were tested for recovery in 2018. Two other departments—Health and Agriculture & Forestry—recorded that only one of their combined 52 critical applications were tested for recovery in 2018. Again, critical information systems supporting essential services are at higher risk of not being recovered as required if disaster recovery plans are not tested regularly.

To monitor the effectiveness of testing, the catalogue tracks how fast an application needs to be recovered based on a department's assessment of existing resource and recovery capability. Based on their last test dates, we found nine critical applications were not recovered within recovery time requirements. One such test occurred in 2013, and there is no indication in the catalogue that a more recent or successful test was performed. We found no evidence of Service Alberta followup with departments to ensure solutions are being worked on and plans exist to retest those applications.

In developing the guidance and requirements for IT disaster recovery, Service Alberta should provide oversight of departments' disaster recovery activities and results. Service Alberta should use the application catalogue to identify where departments are not meeting the policy requirements and to follow up with them on how they will rectify that non-compliance. This oversight process will be fundamental to government's planned centralization of most government IT services in Service Alberta that is currently underway.

Service Alberta provided us with an example of a monthly report it generates from the catalogue. This report lists information for all applications assessed as critical. Service Alberta sends this report to departments; however, we found no targeted followup process with departments on deficiencies related to disaster recovery plans, testing dates, or testing results. As a result, the Minister of Service Alberta cannot state to Albertans that the government disaster recovery plans for critical government IT applications are complete, adequate, and periodically tested.

REPEATED RECOMMENDATION:
Improve recovery of critical information technology applications

We again recommend that the Department of Service Alberta:

- identify the most critical IT applications throughout all government departments
- identify the timelines, after a disaster, that critical IT applications must be recovered
- ensure that there are tested plans and adequate resources to recover critical IT applications within those timelines

Consequences of not taking action

The government may not be able to deliver essential services and programs promptly in a disaster.

Audit Responsibilities and Quality Assurance Statement

Service Alberta, through the Corporate Information Security Office (CISO), is responsible for the IT disaster recovery program, including coordinating and providing IT disaster recovery services for government departments.

Our responsibility is to express an independent conclusion on whether Service Alberta has effective oversight of those departments to ensure that all critical IT applications can be recovered within targeted timelines.

We conducted our audit in accordance with Canadian Standard on Assurance Engagements 3001 issued by the Auditing and Assurance Standards Board (Canada). The Office of the Auditor General applies Canadian Standard on Quality Control 1 and, accordingly, maintains a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements. The office complies with the independence and other ethical requirements of the Chartered Professional Accountants of Alberta Rules of Professional Conduct, which are founded on fundamental principles of integrity and due care, objectivity, professional competence, confidentiality, and professional behaviour.

Auditor General
OF ALBERTA

oag.ab.ca

Contact us:
info@oag.ab.ca
780.427.4222

ISSN 1919-4242 (print)
ISSN 1927-9604 (online)

Making a difference in the lives of Albertans.