Service Alberta—IT Disaster Recovery Program

SUMMARY

On July 11, 2012, a fire in the Shaw Court building in Calgary rendered the data centre located in the building unusable. As a result, many organizations that relied on IT services from this data centre were unable to carry on their normal operations. Among those affected were oil companies, radio stations, and Government of Alberta entities. Although all the government entities using that data centre had disaster recovery plans,[1] they were still unable to provide all the programs and services they expected to within expected times.

Alberta Health Services was unable to access the electronic patient health records in order to provide the necessary healthcare services—i.e., electronically order lab or other diagnostic tests, electronically chart results or notations, and electronically order medications. ATB Financial was unable to provide customer care through its call centre. ATB's online banking, electronic fund transfers and ability to accept some loan applications were also unavailable for up to three days after the incident. Government services such as driver's licenses, land titles, and birth, death and marriage documents were also unavailable.

During and after the Shaw Court fire no coordinated group within government was able to clearly state to Albertans:

- what went wrong
- what was being done to return IT applications to service
- that the government had a clear plan to recover the most critical applications, based on risk and cost, and that it might mean some IT applications may not be available

What we found

It is now two years since the fire at the Shaw Court building. The individual government entities we assessed have better disaster recovery capabilities as a result of identifying and fixing weaknesses in previous disaster recovery plans. However, if a similar incident occurred today, the government would still be unable to say it knows what the most critical government-wide IT applications are, or that it has well-designed and tested plans and the needed resources to recover them within targeted times.

[1] The Alberta Emergency Management Agency defines disaster recovery as the strategies and plans for recovering and restoring government's technological infrastructure and capabilities after a serious interruption and disaster recovery preparedness or plans as the activities associated with continuing availability and restoration of IT infrastructure.

What needs to be done

The Government of Alberta needs to:

- identify its critical programs and services government-wide, and the IT applications that support them
- make government-wide decisions of needed recovery times for critical IT applications and the order they should be recovered based on need, risk and cost
- ensure that the critical IT applications have well-designed and tested recovery plans, and the resources needed to recovered them within those targeted recovery times

Why this is important to Albertans

Albertans expect and rely on government departments, agencies, boards and commissions to provide programs and services. Many of the services unavailable in July 2012 were inconveniences or caused a loss of revenue to the government or other companies in Alberta. However, the sudden absence of some programs and services increased the risk to the safety and well-being of Albertans. To ensure critical programs and services are available when needed, the government should have an effective process to make government-wide decisions on what IT applications must be recovered and when. These decisions should be based on need, risk and reasonable costs. This may mean that during or after a disaster some government programs and services are available sooner than others.

AUDIT OBJECTIVE AND SCOPE

Our audit objective was to determine if the Government of Alberta and its agencies, boards and commissions now have effective systems and processes to:

- identify all of the IT applications in government and the IT applications needed to provide critical programs and services to Albertans
- determine the targeted times for recovering critical IT applications during or after a disaster, based on need, risk and reasonable cost
- ensure there are well-designed and tested recovery plans and the necessary resources to recover critical IT applications throughout the government within targeted recovery times

We selected three of the government entities that were adversely affected by the July 2012 fire in the Shaw Court data centre. These were Alberta Health Services, ATB Financial and the Department of Service Alberta. Service Alberta's inability to provide services impacted other departments that rely on those services. We assessed the work they have completed since July 2012 to fix the weaknesses in their disaster recovery capabilities.

Timing and extent of audit work and auditor responsibilities

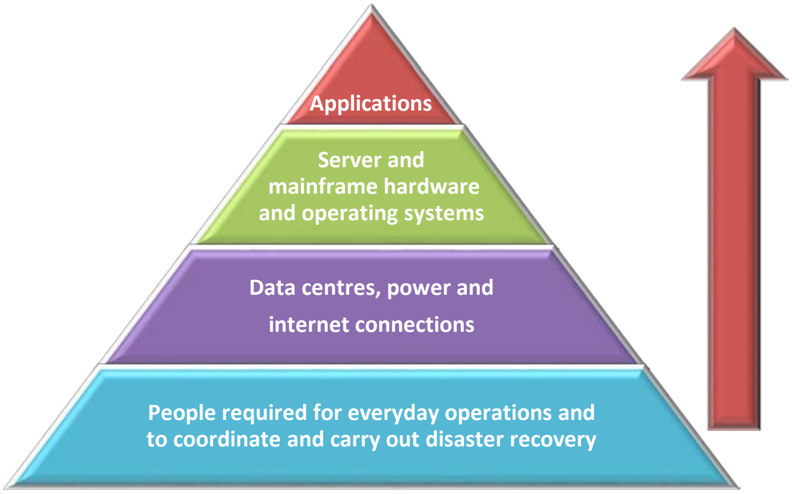
We conducted our field work between January 2014 and July 2014. We substantially completed our audit on July 30, 2014. Our audit was conducted in accordance with the *Auditor General Act* and the standards for assurance engagements set by the Chartered Professional Accountants of Canada.

BACKGROUND

Information technology has become an indispensable component in the delivery of programs and services to Albertans. Government ministries and their agencies, boards and commissions increasingly rely on IT to deliver programs and services Albertans expect and rely on more efficiently, effectively, and economically. A March 2013 project initiated by Service Alberta identified 120 critical and 166 vital IT systems[2] in government departments.

Effective IT disaster recovery involves preparing for major service disruptions before they happen. IT disaster recovery plans usually use business impact or IT risk assessments to prioritize the recovery of critical systems. This helps ensure that critical business information systems are up and running as quickly as possible after a disaster, thereby minimizing disruptions in business activities and services.

To recover from a disaster or significant disruption in service, the data centre environment (for example, electrical power, air cooling and network connectivity to other locations) must be operational and safe before the IT infrastructure[3] can be returned to service. Once the three essential layers of disaster recovery – people, data centres and hardware – are available and operational, then the IT applications can be re-installed or restored to operation.


Applications
Server and mainframe hardware and operating systems
Data centres, power and internet connections
People required for everyday operations and to coordinate and carry out disaster recovery

There are many different groups involved in disaster recovery efforts; for example, data centre owners, IT groups, applications owners and users. Therefore, it is important to know what to do and when to do it, and in what order it must be done to effectively recover IT applications after a disaster. Effective and clear communication and knowledge of the disaster recovery plans is essential to ensure services are returned to normal as soon as possible. However, this is further complicated within government when data centres and the IT infrastructure within them are owned or administered by different departments or third party service providers.

[2] The Alberta Emergency Management Agency defines critical systems as those needing to be recovered within 24 hours and vital systems as those needing to be recovered within 72 hours.

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

FINDINGS AND RECOMMENDATIONS

After the July 2012 disaster the three entities we assessed reviewed what happened, to determine what went wrong and what they needed to improve. Each organization's review identified areas for improving their IT disaster recovery capabilities. All three entities also identified their business critical IT applications and the times they needed to be recovered within to provide critical programs and services. All three entities also developed plans to remediate the weaknesses in their disaster recovery abilities.

Findings at AHS and ATB

Alberta Health Services and ATB both rely on IT to provide efficient and effective programs and services to their stakeholders. The loss of some IT functionality during the July 2012 disaster reaffirms the need for AHS and ATB to ensure critical IT applications are available when and where needed.

AHS is still consolidating the IT infrastructure and applications from the 12 individual health organizations that preceded AHS's formation in 2009. In workshops with its various clinical, business and IT groups, AHS identified their 19 critical applications and the IT infrastructure they need to provide their programs and services. AHS also identified the targeted recover times those systems must be restored and returned to operation within.

We confirmed there are approved plans to obtain the IT infrastructure needed to allow AHS to meet its targeted recovery times. IT disaster recovery plans are also being incorporated into its province-wide IT strategy to consolidate and improve the functionality and availability of those 19 applications. However, without the needed IT infrastructure and disaster recovery plans AHS would currently be unable to recover its critical IT applications within its own targeted recovery times.

We are not making a recommendation to Alberta Health Services at this time, as it is actively consolidating and improving its IT infrastructure so it can meet the targeted recovery times for its 19 critical systems. AHS will provide us with a detailed plan and timelines to implement its IT infrastructure and then to develop and test its disaster recovery plans. We will follow up with AHS in one year to ensure it has met its disaster recovery preparedness deadlines.

ATB updated and broadened its IT disaster recovery plans. These plans include business critical IT applications that did not previously have formal disaster recovery plans. ATB also developed individual technical recovery plans for each of its business critical IT applications.

We are not making a recommendation to ATB at this time, as it is relocating its IT infrastructure out of the Shaw Court data centre and into a new data centre. ATB will test parts of its technical recovery capabilities during the relocation and plans to conduct a full IT disaster recovery test within 12 months of its data centre relocation. We will follow up with ATB next year to ensure that it fully tested its disaster recovery plans

Findings at the Department of Service Alberta

The Department of Service Alberta has two distinct IT groups within it. One group is responsible for administering and providing IT applications for services that Albertans use such as land titles, driver's licenses and birth, death and marriage related documents. The other group, Service Modernization, is responsible for providing core IT infrastructure and applications used by most departments and some of their agencies, boards and commissions.

Service Modernization has improved its disaster recovery plans and capabilities for the core IT infrastructure services it provides to other government departments and organizations. We confirmed that it updated and tested its disaster recovery and technical recovery plans. Those actions also fulfilled a recommendation we made to Service Alberta in 2009.

IT disaster recovery throughout government

RECOMMENDATION 5: IMPROVE RECOVERY OF CRITICAL INFORMATION TECHNOLOGY APPLICATIONS

We recommend that the Department of Service Alberta, with support from the Deputy Ministers' Council:

- identify the most critical IT applications throughout all government entities
- identify the times, 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 times

Criteria

The Government of Alberta should have effective systems and processes to:

- perform or obtain business impact or risk assessments for IT applications from all ministries, including their agencies, boards and commissions
- define the targeted recovery times needed for each IT application based on need, risk and cost
- ensure there are adequate plans and resources to recover IT applications within the targeted times
- inform Albertans, in the event of a disaster, that the most critical IT applications are being recovered according to tested plans and within targeted times

Our audit findings

KEY FINDINGS

There is no one group within the Government of Alberta that has the authority to:

- identify the most critical IT applications throughout government and define the targeted times they need to be recovered after a disaster
- ensure those critical IT applications have well-designed and tested recovery plans and the necessary resources to recover critical IT applications within targeted recovery times
- ensure there are clearly defined communication and coordination procedures for recovering IT infrastructure and applications during a disaster
- inform Albertans in the event of another disaster that the most critical IT applications, based on need, risk and reasonable costs, are being recovered according to defined and tested plans

The Alberta Emergency Management Agency is responsible for ensuring that all departments have updated business continuity plans.[4] As a part of this process AEMA provides business impact assessment templates that departments must complete and return to AEMA. These business impact assessments require departments, but not their agencies, boards or commissions, to identify their critical and vital IT applications. Critical and vital applications must be recovered within 24 and 72 hours respectively. Some departments or their agencies, boards or commissions may have IT applications that need to be recovered in less than 24 hours, but there are currently no requirements to identify them.

[4] Business continuity is the process of identifying how business operations will continue under adverse conditions such as when critical and supporting technology is not available.

The Service Modernization group has tested its ability to restore its core IT infrastructure and has done so in less than 24 hours. However, the recovery of IT applications is the responsibility of each department and their agencies, boards and commissions. Government organizations using Service Modernization's core IT infrastructure must wait for it to finish the recovery of its core services before they can start the recovery of their IT applications.

The recovery of IT applications is then performed by the department itself or with help from Service Modernization. The recovery of IT applications is done on a best effort basis meaning that there is no formal process as to which IT applications are recovered or assurance that IT applications will or can be recovered within needed recovery times.

Service Modernization has developed disaster recovery standards and templates and communicated them to other departments. But no one ensures that departments or their agencies, boards and commissions properly use them or have the planning and resources in place to ensure critical IT applications are available when needed. Further, there is a lack of ability for departments to test their disaster recovery capabilities to recover their IT applications with Service Modernization's core IT infrastructure.

Many different government groups are involved in recovering and restoring critical IT applications during or after a disaster. We did not find defined communication and coordination protocols between these different groups for disaster recovery. Further, there is a lack of a government-wide process or comprehensive plan to determine what are the most critical IT applications to the government and Albertans and to ensure they are available when needed.

This is where we found what we consider to be the biggest risk to the government. Each department and its agencies, boards and commissions, are responsible for ensuring they can recover and restore their own IT applications. Some departments and their agencies rely on Service Modernization or other departments for all or some of their IT infrastructure and disaster recovery capabilities. Other departments and most agencies, boards and commissions use third parties or have their own disaster recovery capabilities.

We found that there is no one group or entity within government with the authority to ensure that critical IT applications the government and Albertans rely on can be recovered within targeted times during or after a disaster. There is no central oversight to:

- identify and rank the importance of programs and services throughout government and the IT infrastructure and applications that support them
- ensure that IT applications supporting critical programs and services have well-designed and tested disaster recovery plans, and the necessary resources so they can be restored when needed
- make decisions and provide assurance that resources for disaster recovery are allocated appropriately
- provide assurance that disaster recovery processes are followed during a disaster

Implications and risks if not implemented

The government may not know what IT infrastructure and applications support critical government programs and services. Therefore, the government may spend more resources than needed in some areas and not enough in others. This also means that the government cannot assure Albertans that:

- it is correctly allocating disaster recovery resources for the right IT infrastructure and applications throughout government
- in the event of another disaster, that IT infrastructure and applications, based on need, risk and cost, are being recovered according to tested plans and within the targeted times