2 Disaster Preparedness – Major Government Information Systems

Summary

The continued operation of critical provincial government information systems could be in jeopardy if a disaster were to occur. This could expose Nova Scotians to risks such as interruption of important government services (e.g., social assistance), loss of critical data (e.g., property and business records), and impaired public safety (e.g., information not being available to the courts, jails and police).

Two groups responsible for the recovery of major provincial government computer systems in the event of a disaster were examined as a part of this audit: the Chief Information Office (CIO) which is responsible for the provincial data centre and most of government's nonfinancial information systems; and the Department of Finance's Corporate Information Systems division (CIS) which is responsible for most of government's financial systems. We found that CIS has a good-quality, thorough disaster recovery plan which has been validated through testing. However, the CIO does not have a comprehensive, up-to-date plan.

In June of 2010, the CIO became responsible for disaster preparedness at the provincial data centre and inherited some disaster recovery documents created when the province's IT operations were decentralized. CIO has since started a project to create a comprehensive disaster recovery plan but, at this time, is not yet fully prepared to restore systems quickly if a disaster impacts the provincial data centre. A current, comprehensive disaster recovery plan has yet to be prepared and there is insufficient other guidance to follow in a time of crisis. Disaster response testing and training have not been performed, and there is no secondary processing site that can handle all of the critical systems hosted by the provincial data centre. We also identified some risks to the data centre which should be mitigated.

CIS is a separate information technology group. Although it uses space at the provincial data centre, it manages its own information systems. We found it has a comprehensive plan that will allow for the restoration of government's financial systems should the provincial data centre become unavailable. CIS's plan is tested regularly and includes the ability to restore systems at a secondary processing site. Nevertheless, our audit identified some areas for improvement in CIS's plan with regard to the proximity of the secondary site to the data centre, the lack of documented procedures to provide network connectivity to the backup systems, and offsite storage of the disaster recovery plan.

2 Disaster Preparedness – Major Government Information Systems

Background

DISASTER PREPAREDNESS – MAJOR GOVERNMENT INFORMATION SYSTEMS

2.1 Information technology disasters are events that adversely impact the availability of computer systems critical to an organization's operations. Examples of such disasters include hacker attacks, building fire, and loss of electricity or building integrity due to a storm. Being prepared for a disaster results in faster, more organized responses to both minor interruptions and major disasters.

2.2 Elements involved in the preparation for a disaster include: storing copies of computer data and software in multiple locations, establishing computer system priorities, identifying human and physical resource requirements, determining data backup and recovery procedures, and defining roles and procedures for preventing and minimizing service interruptions. All of the information and instructions needed to recover from a disaster are documented in a disaster recovery plan and include areas such as a business impact analysis; system inventories and priorities; incident response plans; contact information; and backup, testing and training strategies. The plan should be validated through regular testing.

2.3 If the Nova Scotia government's computer systems were impacted by a disaster, they could become unavailable for an extended period of time if the government is not adequately prepared. Important government services and operations that rely heavily on computers include providing social assistance payments; operating the provincial jails and courts; recording patient information at hospitals; providing permits needed to start up new businesses; and maintaining records vital to buying and selling property. Even with contingency plans in place to provide some critical services without the aid of computers, Nova Scotians would be affected.

2.4 The majority of systems in use throughout the Nova Scotia government are located at the provincial data centre. The data centre provides the physical space, computer equipment, operating systems and other infrastructure required to run applications throughout government. The data centre also supports government-wide services such as email and network connectivity.

DISASTER PREPAREDNESS – MAJOR GOVERNMENT INFORMATION SYSTEMS

2.5 Most of the provincial government information systems are supported by three groups: Chief Information Office, Corporate Information Systems and Health Information Technology Services Nova Scotia.

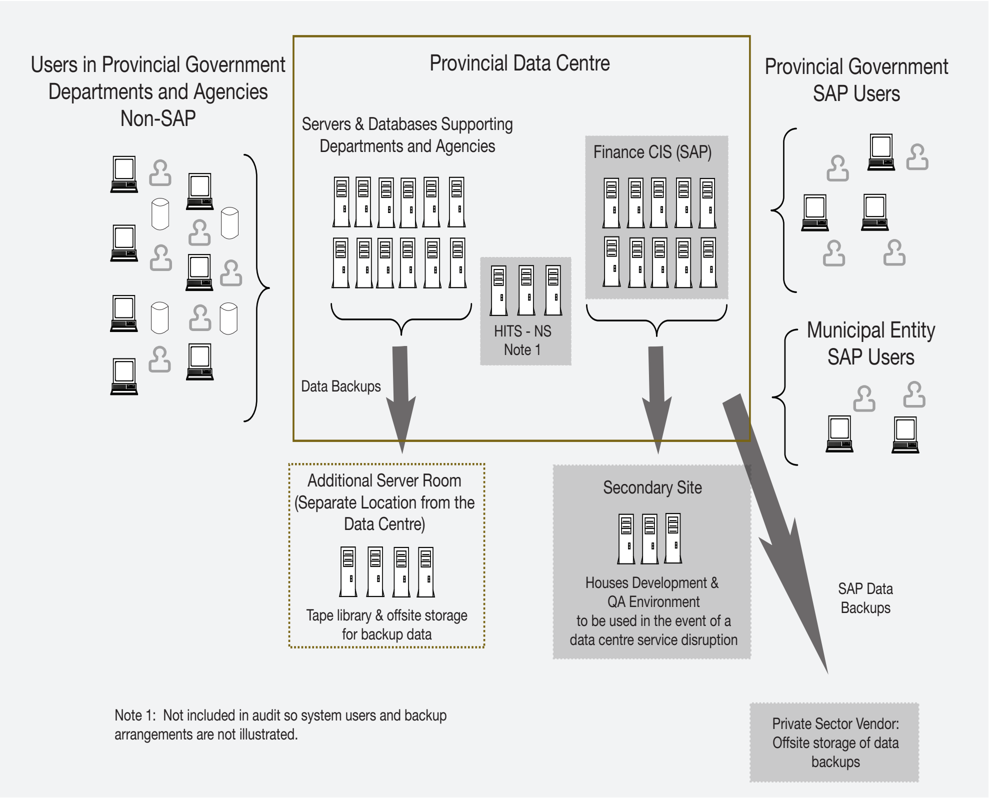
2.6 The Chief Information Office (CIO) supports the infrastructure that hosts mostly nonfinancial computer systems operated by provincial government departments and agencies (e.g., registry of motor vehicles). The CIO is responsible for managing the provincial data centre and any related disaster preparedness.

2.7 Corporate Information Systems (CIS), a division of the Department of Finance, is responsible for supporting the government's corporate financial management systems. Government uses the computer application SAP to process the majority of its financial transactions. SAP is used for processes such as government accounting, budgeting, human resources/payroll, and payments for goods and services.

2.8 CIS also supports several instances of SAP used by other provincial and municipal government entities: regional school boards, district health authorities, regional housing authorities, Nova Scotia Liquor Corporation, certain municipalities, and the Halifax Regional Water Commission. SAP servers and databases are housed at the provincial data centre. However, CIS has its own personnel to manage the SAP systems and the development and maintenance of its disaster preparedness.

2.9 Health Information Technology Services Nova Scotia (HITS-NS) houses its servers and databases at the data centre. This organization is fully funded by the Department of Health and Wellness and is mandated by the Department to provide centralized support of provincial health IT operational systems. It relies upon the data centre to be available, but is responsible for its own disaster preparedness. We did not examine the state of disaster preparedness at HITS-NS as part of this audit, but will do so in a future audit of electronic health records.

2.10 The following diagram illustrates the relationship of the infrastructure managed by CIO, CIS and HITS-NS to the provincial data centre.


Users in Provincial Government Departments and Agencies Non-SAP
Provincial Data Centre
Servers & Databases Supporting Departments and Agencies
Finance CIS (SAP)
HITS - NS Note 1
Data Backups
Provincial Government SAP Users
Municipal Entity SAP Users
Additional Server Room (Separate Location from the Data Centre)
Tape library & offsite storage for backup data
Secondary Site
Houses Development & QA Environment to be used in the event of a data centre service disruption
SAP Data Backups
Private Sector Vendor: Offsite storage of data backups

Note 1: Not included in audit so system users and backup arrangements are not illustrated.

Audit Objective and Scope

2.11 In the summer of 2011 we completed an audit of disaster preparedness related to systems hosted by the provincial data centre and to government's corporate financial management systems. The objective of the audit was to determine if, in the event of a disaster or other service interruption at the provincial data centre, the government is capable of an orderly and timely recovery of information technology processes required to support government programs and services important to the safety and wellbeing of Nova Scotians.

2.12 Most of our audit fieldwork was conducted during May and June 2011, and focused on the disaster preparedness of the two groups responsible for most of the systems physically housed by the data centre: the Chief Information Office and Corporate Information Systems. We did not include systems managed by Health Information Technology Services Nova Scotia because we plan to examine them in a future audit. Our audit also did not include assessing the business continuity plans of the various government departments that have systems supported by the data centre. Business continuity planning addresses how an organization will maintain critical operations during the period of time that computer systems are not available.

2.13 This engagement was conducted in accordance with Sections 18 and 21 of the Auditor General Act and auditing standards established by the Canadian Institute of Chartered Accountants. Audit criteria were based on the IT Governance Institute's framework, Control Objectives for Information and related Technology (COBIT 4.1), which is a widely-accepted international source of best practices for the governance, control, management and audit of information technology operations. Our audit objective and criteria were discussed with, and accepted as appropriate by, senior management of the Chief Information Office and Corporate Information Systems.

Significant Audit Observations

Disaster Preparedness at the Chief Information Office

Conclusions and summary of observations

The Chief Information Office (CIO) is not prepared to quickly recover from a disaster impacting the provincial data centre. It does not have a thorough, up-to-date disaster recovery plan to execute. Preparation of a plan is in progress and the CIO has taken steps to mitigate some of the known risks to the data centre. However, documents available to provide guidance in a time of crisis are inadequate; disaster response testing and training have not been done; and there is no secondary processing site that can handle all of the critical systems hosted by the provincial data centre. Unmitigated risks to the data centre were identified that could increase the possibility of needing to activate a disaster recovery plan. If a disaster were to occur, information systems critical to public safety and wellbeing may not be restored quickly and effectively.

2.14 *Disaster recovery plan preparation* – In June of 2010, the CIO became responsible for disaster preparedness at the provincial data centre and inherited some disaster recovery documents created when the province's IT operations were decentralized. Since then, the CIO has started a major project which will result in the preparation of a comprehensive disaster recovery plan. Management informed us that they are using a framework from the British Standards Institute as their guide. We reviewed the disaster recovery project plan and concluded that the plan and the framework contain the critical elements we would expect to see in such documents.

2.15 The importance of having a well-documented, up-to-date and tested disaster recovery plan cannot be overstated. The CIO does not have a plan that meets those criteria. According to the project plan to prepare the disaster recovery plan, the CIO has passed the target completion date of March 31, 2011 and a new target has not yet been set. Every effort should be made to complete this project as soon as possible.

Recommendation 2.1
The Chief Information Office should complete its disaster recovery plan as soon as possible without jeopardizing the completeness and quality of the plan.

2.16 *Secondary site* – Disaster recovery strategies typically include a secondary site to restore critical computer systems in the event of a disaster. The CIO does not have sufficient facilities to restore systems at a secondary site if the provincial data centre becomes unavailable. The CIO's secondary site is a server room in another building where its data backup tapes are currently stored. However, its capacity is limited and it would not be capable of supporting the number of critical government systems that would need to be established there.

2.17 The secondary site is also located too close to the provincial data centre and is susceptible to threats that impact a wider area (e.g., power outages).

2.18 CIO management informed us that, as part of its strategic vision, they will be issuing Requests for Expression of Interest from vendors in fall 2011 to develop an information processing solution that involves two separate data centres. A secondary site strategy is still necessary for the interim period.

Recommendation 2.2
The Chief Information Office should establish and implement a strategy that provides restoration facilities in the event the provincial data centre becomes unavailable.

2.19 *Disaster preparedness* – A disaster recovery plan communicates the various responsibilities, processes and resources required to recover from a disaster in a timely and effective manner. However, in its absence, it is still critical to have guidance and processes to assist during a disaster. We reviewed the state of the CIO's disaster preparedness and found that it does not address all the elements that would enable a timely and complete recovery from a disaster.

2.20 The CIO has not worked with its client departments and agencies to complete a business impact analysis or threat risk assessment. It is difficult to be prepared for a disaster if it is not clear which threats are plausible and how they may impact the operation of the data centre and government.

Such analysis is needed before the following decision-making tools can be completed.

- A complete inventory of resources necessary (e.g., human, hardware, software, etc.) to restore systems is required because trying to identify those resources during a crisis would hinder the ability to recover in a timely manner.
- Identification of system priorities is necessary as it determines the order in which systems should be shut down or restored in the event of a disaster.

Recommendation 2.3
The Chief Information Office should complete a business impact analysis and threat risk assessment in conjunction with its client departments and agencies to assist in the documentation of information system requirements and priorities in the event of a disaster.

2.21 The CIO has a documented crisis management plan and guidance for declaring a disaster. However, these incident-handling procedures are documented at a high level. The knowledge and experience of key staff members are needed to assess and manage such incidents. If those staff members are unavailable, the procedures may be implemented ineffectively. For example, if the data centre coordinator was unreachable during a disaster, potentially valuable time would be lost even if a data centre coordinator from outside the organization was available. Without documentation, the outside coordinator would need to take time to become familiar with the specifics of the provincial data centre.

Recommendation 2.4
The Chief Information Office should ensure documented disaster recovery procedures are sufficiently detailed to avoid reliance on specific staff members.

2.22 *Testing* – Currently, management cannot ensure it can recover systems after a disaster because there has not been any testing of the processes that would be followed. A test of a disaster recovery plan and processes generally involve making systems unavailable for a limited time and requiring staff to perform the disaster recovery procedures as defined.

Recommendation 2.5
The Chief Information Office should test the procedures defined to recover from a disaster.

2.23 *Training* – Training has not been provided to staff expected to be involved in the disaster recovery process. Failure to train staff on processes and lessons learned increases the risk that mistakes will be made during the mitigation and recovery phases of a disaster. This could increase the negative impacts of a disaster or the time required to recover.

Recommendation 2.6
The Chief Information Office should develop a training strategy and provide training on the processes used to recover from a disaster.

2.24 *Data backup* – Procedures for the regular backup and recovery of data are critical to the success of a disaster recovery strategy. We saw evidence that the data centre regularly performs data backups. The data is sent electronically in a secure manner to a tape library in another building used by the provincial government. However, we found that data backup policies and processes are not documented.

2.25 Due to the lack of documented guidance, backup and restoration is dependent on the skills of specific individuals. If those key staff members are unavailable during a disaster, successful recovery is at risk.

Recommendation 2.7
The Chief Information Office should document data backup policies and procedures.

2.26 *Agreements* – The Department of Transportation and Infrastructure Renewal manages the physical aspects of the building that houses the provincial data centre. Building services such as server room cooling, power supply and backup generators are critical factors in the functioning of the data centre and those services should be clearly defined. There is no written agreement between the CIO and the Department of Transportation and Infrastructure Renewal for the level of services that can be expected during, or immediately subsequent to, a disaster impacting the data centre. This could lead to increased downtime of critical systems in a time of crisis.

Recommendation 2.8
The Chief Information Office should ensure all services it receives that are necessary to protect and operate the data centre are covered by a written agreement.

2.27 *Physical risks to the data centre* – The CIO has undertaken a significant overhaul of the data centre based on the results of various assessments that were performed over the past few years. These assessments reviewed physical attributes of the data centre such as security, backup power and fire suppression. Improvements will result in a more reliable and stable data centre that is less susceptible to service interruptions.

2.28 We observed two areas of heightened risk to the continued operation of the provincial data centre.

- The data centre's server room is located directly above a records warehouse. This warehouse contains boxes of paper records that are stacked from floor to ceiling. This increases the risk of damage to the data centre from fire.

- The building facilities for the data centre do not use a gas-based fire suppression system. The use of water-based fire suppression can damage computer equipment if it is activated, whether in a fire emergency situation or due to malfunction. We noted that the data centre's secondary site does employ a gas-based fire suppression system.

Recommendation 2.9
The Chief Information Office should separate the data centre from the paper records warehouse.

Recommendation 2.10
The Chief Information Office should evaluate the cost and benefits of a gas-based fire suppression system in its current and future data centres.

Disaster Preparedness at Corporate Information Systems

Conclusions and summary of observations

The Corporate Information Systems (CIS) division of the Department of Finance has a comprehensive disaster recovery plan for the SAP applications it supports. The plan is regularly tested and includes the ability to restore the applications at a separate backup facility should the provincial data centre become unavailable. Our audit concluded that most of the critical areas of a disaster recovery plan were addressed. Our audit also identified a few areas for improvement, including the proximity of the secondary site to the data centre, the lack of documented procedures to provide network connectivity to the backup systems, and not storing the disaster recovery plan offsite.

2.29 *Disaster recovery plan* – A disaster recovery plan has been created by CIS. This plan covers the financial applications CIS manages for the Nova Scotia government, as well as the other SAP clients supported by CIS. Our review of the plan indicated that it addressed most of the areas that are necessary for an adequate plan. Priorities and resource needs in a disaster scenario are documented and linked to risk assessments. We found ongoing stakeholder input and annual testing of the plan. We also saw evidence of appropriate backup procedures being followed.

2.30 *Location of secondary site* – CIS has an active secondary site it can use if the provincial data centre becomes unavailable. This facility is referred to as a hot site because the infrastructure and backup data is already in place for use by CIS and its clients whenever needed. The CIS disaster recovery plan notes that disasters occurring within a 3.2 kilometer radius around the provincial data centre could require moving to the secondary site. The distance between the data centre and the secondary site is approximately two kilometers. As a result, the secondary site is at risk of being unavailable during a disaster which affects a wider area.

2.31 As noted above, the CIO is currently developing a strategy that involves the use of two separate data centres. Discussions with CIS indicated that they have plans to re-evaluate their current secondary location once the CIO implements their new data centre strategy. The long-term plan is to use the CIO's data centres if they fit the requirements of CIS and its clients. In the short term, CIS needs to evaluate the risk to operations of having the two processing sites within their defined radius of 3.2 kilometers.

Recommendation 2.11
Corporate Information Systems should perform an assessment to identify key threats and the impact of a disaster affecting both the primary and secondary data centre sites simultaneously.

2.32 *Accessibility of restored systems* – Hundreds of SAP users access the system through the provincial wide-area network. The secondary site used for SAP systems relies on the provincial data centre to connect to the provincial network. In the event the data centre was impacted by a disaster and the connection was lost, most SAP users would be unable to access the backup SAP system.

2.33 The secondary site has the network infrastructure needed to connect SAP users to their systems, but CIS has not documented the steps necessary to establish that connection. Therefore, SAP users are at risk of being unable to access SAP and resume business activities, even though the SAP software and data have been restored at the secondary site. The procedures to obtain and configure alternate network access should be included in CIS's disaster recovery plan to reduce downtime in the event the provincial data centre becomes unavailable.

Recommendation 2.12
Corporate Information Systems should include procedures required to establish alternate means of network connectivity in its disaster recovery plan so SAP users can access systems at the secondary site.

2.34 *Relationship with secondary site owner* – CIS does not own the building that houses the secondary site. It rents the space needed for its servers from another government entity. However, this business arrangement has not been formalized. There is no written agreement defining service levels that would be provided if there is a disaster that affects both the provincial data centre and the secondary site.

Recommendation 2.13
Corporate Information Systems should execute a written agreement for the supply of space and services needed to operate the SAP secondary site.

2.35 *Distribution of the disaster recovery plan* – It is a best practice to maintain a current copy of a disaster recovery plan offsite to ensure it is accessible in the event that a primary facility or network becomes unavailable. The SAP disaster recovery plan outlines procedures for its communication, distribution and offsite storage. There was no evidence that this was happening as intended.

2.36 We did not find evidence of a physical copy of the SAP disaster recovery plan offsite. We were informed that a member of CIS management stores an electronic copy of the plan offsite. Without an easily accessible plan, critical recovery procedures may be delayed or missed, causing confusion and delays in restoring systems and data.

Recommendation 2.14
Corporate Information Systems should take steps to ensure the communication and distribution procedures of the SAP disaster recovery plan are followed.

2.37 *Disaster recovery training and lessons learned* – Training and steps to evaluate lessons learned after execution of the disaster recovery plan are important elements of disaster preparedness. Informal training was evident through CIS's annual disaster recovery testing activities. However, the plan itself does not include training and awareness procedures or steps to evaluate lessons learned. Without consistency around training and debriefing of annual test results, staff members may not be completely aware of their roles, responsibilities and procedures in the event of a disaster.

Recommendation 2.15
Corporate Information Systems should include procedures with respect to training, awareness and lessons learned in its SAP disaster recovery plan.

RESPONSE:
CHIEF
INFORMATION
OFFICE

Response: Chief Information Office

The Chief Information Office would like to thank the staff of the Auditor General for their courtesy and professionalism while conducting this audit.

The Office recognizes the critical importance of information technology-based services and resources to both government and the citizens it serves. The Office accepts the recommendations presented and is pleased that the priorities and activities of the Office to date align with the areas this audit report highlights.

The Chief Information Office took on responsibility for corporate information technology infrastructure from the Corporate Service Units and Corporate IT Operations in June 2010. As a result, one of the first priorities of the Office was to assess government's disaster recovery status and to aggressively work to increase the resilience and sustainability of its information technology assets and services.

Significant investments have been made to date and risks mitigated. A team of disaster recovery specialists is currently being created to solely focus on this critical area of our operations. A governance Risk Committee has been constituted in the last year to evaluate and recommend mitigation options around risks to government's IT assets. The Office has an interim Disaster Recovery Plan in place and will be completing the next refinement of the plan for the late fall. Also this fall, the Office will be releasing a Request for Information to gather vendor input into how government could competitively procure a secondary data centre that would enhance disaster recovery preparedness.

Although the Office has held the disaster recovery portfolio for a short time, significant progress has been made and much more will be accomplished in the coming years. We look forward to further demonstrating our commitment to continuous improvement in the area of disaster recovery.

Response: Department of Finance – Corporate Information Systems

Thank you for the opportunity to review and respond to the draft of Chapter 2 – Disaster Preparedness – Major Government Information Systems in your November 2011 report. We offer the following comments, which may be included in your report as the response of the Corporate Information Systems division in the Department of Finance.

Recommendation 2.11
Corporate Information Systems should perform an assessment to identify key threats and the impact of a disaster affecting both the primary and secondary data centre sites simultaneously.

Management agrees with this recommendation. Although an informal risk assessment was completed during the initial selection of the secondary site, a formal risk assessment could provide additional information that would assist in managing various disaster recovery scenarios.

The secondary site is located within a facility that houses other critical government services and therefore, would be a priority for power restoration and accessibility (two major factors in determining location risk) during a disaster scenario.

As stated in the report, the location of the secondary site will be re-evaluated as part of the data centre strategy being developed by the CIO.

Recommendation 2.12
Corporate Information Systems should include procedures required to establish alternate means of network connectivity in its disaster recovery plan so SAP users can access systems at the secondary site.

Management agrees with this recommendation. The steps to re-establish network connectivity to the secondary site for SAP end users will be documented in the disaster recovery plan.

Recommendation 2.13
Corporate Information Systems should execute a written agreement for the supply of space and services needed to operate the SAP secondary site.

Management agrees with this recommendation. However, it should be noted that the secondary site and services are provided by another major government agency and a successful informal arrangement has been in place for several years. The secondary site is fully operational at all times for development and quality assurance systems, so no additional space or services are required in the event provisions of the disaster recovery plan are invoked. This same government agency also uses SAP systems to provide critical services such as HR/Payroll, so

RESPONSE: DEPARTMENT OF FINANCE – CORPORATE INFORMATION SYSTEMS

RESPONSE: DEPARTMENT OF FINANCE – CORPORATE INFORMATION SYSTEMS

it is also unlikely that any space or services would be withheld during a disaster recovery event.

Recommendation 2.14
Corporate Information Systems should take steps to ensure the communication and distribution procedures of the SAP disaster recovery plan are followed.

Management agrees with this recommendation.

Recommendation 2.15
Corporate Information Systems should include procedures with respect to training, awareness and lessons learned in its SAP disaster recovery plan.

Management agrees with this recommendation. Informal training occurs as a result of execution of the test procedures associated with the disaster recovery plan. Lessons learned are also incorporated each year in the revised disaster recovery plan. These activities will be formally documented in the plan to ensure verification that a continuous improvement process is in place.