Report 1: April 2010

IT CONTINUITY PLANNING IN GOVERNMENT

www.bcauditor.com

OFFICE OF THE
Auditor General
of British Columbia

Library and Archives Canada Cataloguing in Publication
British Columbia. Office of the Auditor General

IT continuity planning in government [electronic resource].

Electronic monograph in PDF format.
Includes index.
Includes bibliographical references and index.

ISBN 978-0-7726-6278-1

1. Administrative agencies--British Columbia--Information resources management. 2. Administrative agencies--Information technology--British Columbia--Management. 3. Administrative agencies--Security measures- British Columbia. 4. Information technology--Security measures--British Columbia. 5. Electronic government information--Security measures--British Columbia. 6. Government communication systems--Security measures--British Columbia. 7. Emergency management--British Columbia--Planning. 8. Data protection--British Columbia. I. Title.

HD30.2 B7 2010 352.3'809711 C2010-902209-2

TABLE OF CONTENTS

AUDITOR GENERAL'S COMMENTS

JOHN DOYLE, MBA, CA
Auditor General

INFORMATION TECHNOLOGY MANAGEMENT

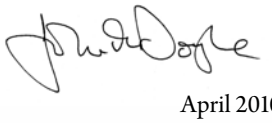
has become a vital component in the delivery of government programs. The Province's reliance on IT has intensified over the last decade as information systems have become more complex and embedded into day-to-day operations. More of government's IT infrastructure is also now managed by third parties.

IT continuity planning involves proactively preparing for major service interruptions such as earthquakes or pandemics. Proper IT continuity planning ensures that the most critical government information systems are up and running as quickly as possible after a disaster, thereby minimizing disruptions in government services. Given that information systems are critical to government operations, IT continuity planning should be a key responsibility of government.

In British Columbia, our provincial government is sufficiently prepared to recover from localized disruptions, such as a temporary power outages or equipment failures. However, many of government's critical systems are housed in shared facilities, and run on shared platforms. While they are physically interconnected, they lack coordination between the systems, and communication between the key ministries and external service providers. In the event of a major disaster, there is no overall strategy for prioritizing the recovery of critical systems.

I am pleased to note, however, that government plans to address my recommendations. Government should not risk losing its tremendous investment and the significant knowledge stored in its IT systems to a disaster, when proactive work now could mitigate this risk.

I would like to thank the staff at Shared Services BC (Ministry of Citizens' Services), Children and Family Services (Ministry of Children and Family Development), BC Ambulance Service (Ministry of Health Services) and Emergency Management BC (Ministry of Public Safety and Solicitor General), for the cooperation and assistance they provided to my staff during this audit.



April 2010

AUDIT TEAM

Bill Gilhooly,
Assistant Auditor General

Faye Fletcher,
IT Audit Specialist

Joji Fortin,
Manager IT Audit

Jenny Wang,
Manager IT Audit

Rolf Goerzen,
Manager

Chris Lawson,
Senior Audit Associate

Cara Bourassa,
Audit Associate

Heather Sharpe,
Audit Associate

EXECUTIVE SUMMARY

In British Columbia, the provincial government increasingly relies on information technology (IT) in a wide range of ways. For instance, IT is used to promote service delivery through e-business, to enable central government and the broader public sector to share information and systems back and forth, and to enhance the ever more complex information systems that support critical programs. A disruption to any of these services and systems – from a large fire, a criminal act, a strong earthquake or any other such emergency or disaster – leading to loss of information or the ability to process information can have extremely serious consequences for government programs.

Effective IT continuity planning aims to minimize the potential consequences of such a disruption. A good IT continuity plan is part of the larger business continuity process that requires several different plans to be in place to prepare for the response, recovery and continuity of government's business.

- The *business continuity plan* outlines procedures to ensure the continuation of business processes, including IT to support those, in the event of an interruption, covering both manual and computerized processes.
- The *IT continuity plan* specifically addresses IT exposures and solutions based on the business priorities set out in a business continuity plan.
- A subset of the IT continuity plan, *the disaster recovery plan,* prepares for major events that result in the relocation of IT processing for an extended period. It does not address minor local disruptions.

Each of these plans can be separate documents, or the IT continuity and disaster recovery plans can be embedded within the business continuity plan.

In considering the potential for service disruptions, government identified certain business functions as "mission-critical," along with the IT applications and supporting systems used to deliver them. Mission-critical business functions were defined as being those that, if not recovered on a timely basis, could result in loss of life, impaired public safety, or personal and financial hardship suffered by the province's citizens. All such functions rely heavily on the continued operation of IT systems to provide the information needed within each function to make decisions, manage resources and deliver services.

An initial government-wide ranking of business functions, prepared in early 2009, identified 49 as "program mission-critical" and 22 as "support mission-critical." We conducted this audit to assess whether the provincial government has adequate processes in place to ensure the continued operation of the IT applications and supporting systems and services that are required to deliver these mission-critical business functions. Samples were selected from the government-wide ranking to determine whether the related business areas had adequately:

- identified risks and prioritized recovery of services;
- developed IT continuity plans that aligned with business continuity plans and government policies;
- ensured that IT recovery plans and processes were remaining appropriate and complete;
- tested IT continuity plans regularly; and
- kept IT continuity plans current.

We issued detailed management reports of our findings to the senior management in each ministry we audited. In this report, we summarize only our high-level key findings and key recommendations.

OVERALL CONCLUSION

In our examination, we found that management in the ministries recognize the importance of planning for disasters and have implemented business continuity management programs. Many best practice procedures are in place within these programs, but improvement in several areas of IT continuity planning would strengthen all business continuity plans.

In all of the business functions we sampled, adequate processes are in place to allow the recovery of critical systems from minor localized disruptions, such as temporary power outages or equipment failure.

The situation is different in the case of a major disaster. Many of government's critical systems run on shared computing environments, housed in shared facilities. Given their interconnection, there is a risk that all of the supporting elements may not be in place to ensure critical systems can effectively be recovered. Two particular weaknesses stand out:

- One is the lack of an overall strategy for prioritizing the recovery of shared systems and program applications. Competing demands for resources by mission-critical government programs during or following a major disaster could result in a serious shortfall between the shared systems required and those available.

- The other is the lack of clarity by each ministry – using dedicated operating environments provided by service providers – about whether the ministry has made the necessary arrangements to ensure that these operating environments can be recovered within the times required to meet the needs of the ministry program area they support.

KEY FINDINGS AND RECOMMENDATIONS

Improvements to identification of risks and prioritization of recovery are needed

- While those in our audit sample used some initial risk assessment and business impact analysis methods to identify and rank service recovery risks, generally no ministry prepared a formal assessment or updated it annually. Doing so is outlined in government policy, with the aim of ensuring that continuity plans stay current and reflect any significant change government makes to its business needs, applications and technology.

- There is no overall strategy for prioritizing the recovery of shared systems and mission-critical program applications. This is a critical gap, as several government programs would be competing for shared system resources in the event of a major disaster. The result could be more shared systems being required than are available.

- In some cases, we found that the recovery times for operating environments and other shared systems do not coincide with the recovery time of the business function that these environments and systems need to support. This poses the risk that the business function will not resume within the required timeline.

- The majority of the infrastructures for shared systems are located in a primary data centre facility in Victoria. Alternate arrangements to continue operations (such as recovery and failover sites and application and data backup facilities) are located in the same geographical area as primary operations and the data centre facility – all are not far from an earthquake fault line. Government has not adequately addressed the potential threat scenario this situation posts

WE RECOMMEND:

- Preparation of a business impact analysis and risk assessments annually, as outlined in government policy

- Prioritization of the recovery of mission-critical applications at the ministry level and across government

- Establishment of realistic and achievable recovery timelines for shared systems and program applications

- Assessment of risk associated with alternate arrangements being in the same geographical area as the primary operations and data centre facility, and feasibility of relocation

Not all critical business functions have IT continuity plans

- A business continuity management program is in place at the ministry level in the audit clients we sampled. However, we found that not all business continuity plans we examined were finalized.

- Formal disaster recovery plans have not been prepared for some network infrastructures and it is unclear whether they have been prepared for certain operating environments. This creates a risk that, in the event of a disaster, these environments and infrastructures may not be restored within timelines required by ministry programs.

WE RECOMMEND:

- Finalization of business continuity plans for all mission-critical business functions

- Preparation of disaster recovery plans to support the availability of significant operating environments and network infrastructures within the timelines required by ministry programs

Processes are not always adequate to ensure IT recovery plans are appropriate and complete, routinely tested and kept current

- For many of the shared systems we reviewed, we found that responsibility for their development, day-to-day operations and maintenance has been contracted to third-party vendors through alternative service delivery agreements. Still, while service delivery has been transferred, accountability remains with the Province, which must ensure that the risks are managed and there is continued delivery of service.

  Where these outsourced arrangements exist, best practice requires that controls be reaffirmed and responsibility to develop, test and execute continuity and recovery plans be clearly identified and assigned. The third-party contracts in our samples included business continuity and disaster recovery requirements. Except for two contracts, they also required testing of business continuity and disaster recovery plans.

  We were informed that some major infrastructure contracts predate the current policy that now requires formal business continuity planning. As these contracts expire or become renewed, the inclusion of business continuity requirements will be brought forward by the negotiating owners. In our view, the situation puts timely recovery of critical processes at risk if a disaster were to occur between now and when these contracts are renegotiated.

- Not all disaster recovery plans examined are being tested routinely, according to government policy, to validate the plans are complete and the logistics work.

- Not all business continuity plans in our sample were updated on an annual basis as required by government policy. This could result in out-of-date restoration processes.

WE RECOMMEND:

- Inclusion, in contracts with third-party providers of critical services, of provisions regarding both the preparation and testing of business and IT continuity plans and the assessment of risks where inclusion of these provisions is not feasible

- Regular testing of continuity plans and restoration procedures for all mission-critical applications and supporting systems

- Updating of business continuity plans for all mission-critical business functions annually

Table 1 shows the number of recommendations we made in our detailed management reports under each key audit area. We discuss our findings in more detail in the following section of this report.

Table 1: Recommendations made under each key audit area

Key audit area	No. of detailed recommendations made
Identifying risks and prioritizing recovery of services	
A continuity framework and policy are in place.	*0*
Business recovery needs and drivers for development of an IT continuity plan are identified.	*16*
Developing IT continuity plans	
An IT continuity plan is established to reflect the business continuity plan.	*9*
Ensuring IT recovery plans are appropriate and complete	
The IT continuity plan is complete and addresses business continuity requirements defined in the business continuity plan.	*16*
Testing IT continuity plans regularly	
The plan is tested regularly with, for example, a comprehensive verification of continuity processes, and situational drills to test the assumptions and alternate procedures within the plan.	*21*
Keeping IT continuity plans current	
The IT continuity plan is maintained to reflect system and application changes as well as modifications to the business continuity plan.	*9*
Total	*71*

GOVERNMENT'S RESPONSE

THIS GOVERNMENT APPRECIATES and supports the key findings and recommendations from the Office of the Auditor General's review entitled IT Continuity Planning in Government. The work of the audit team will assist the Province with its ongoing efforts to improve business and IT continuity planning across government.

We are pleased with the team's conclusion that all of the business functions sampled were prepared for localized disruptions. This would include events ranging from temporary power outages and equipment failure to floods and fires, which the Province deals with on a regular basis. We are addressing the team's recommendations to further enhance and improve existing systems to ensure government is better prepared to recover from the very rare, but more severe, business disruptions associated with a major disaster such as a large earthquake.

In 2009, government began implementing a more formal prioritization of IT recovery sequencing – which IT systems need to be made operational first in the event of a major disruption – and this work is expected to be complete in 2010. In addition, Shared Services BC has implemented a new formal process for ministries to ensure IT system Recovery Time Objectives – how quickly business functions need to be made operational – are aligned with business requirements. Shared Services BC will continue working with ministries over the next year to improve awareness of hosting services that are available to them to provide additional redundancy, failover, and geographic distribution for business applications that require added availability.

To ensure the continuous operation of government's mission-critical applications, in March 2009, Shared Services BC entered into a service provider agreement with Advanced Solutions, an HP Company, that will see the government's 2,000 computer servers at the Province's Data Centre moved from current locations in Victoria and Vancouver to, new redundant data centres in alternate locations. These new locations are outside of the geographic area at high risk of earthquake, and outside of the local 200 year flood plain for their areas. This process will be phased-in over the next five years to avoid any service disruption.

These efforts to improve IT continuity planning across government are consistent with work already completed or underway to enhance government's overall business continuity planning for major disasters including:

- Introduction of a Concept of Operations for Business Continuity document and the first ever cross-government exercise specifically targeting business continuity major disasters – November 2009.
- Introduction of revised tools and additional training to enhance ministry planning – March 2010.
- Increased reporting by ministries regarding the status of their business continuity plans and exercise programs – Implementation by December 2010.
- Updates to the Core Policy for Business Continuity, to clarify accountabilities and requirements which will facilitate ministry planning – Implementation by December 2010.

Overall, the audit team's recommendations reflect existing and proposed Core Policy for Business Continuity, and existing business continuity enhancement objectives within ministries, and across government. The report will assist government in focussing work already underway to enhance business continuity for major disasters.

BACKGROUND

What is IT continuity planning?

Information technology (IT) continuity planning is a vital part of business continuity planning.

A business continuity plan outlines the procedures and instructions an organization needs in place to ensure that its business processes will be able to continue if interrupted, whether by a minor localized disruption (such as a power outage or equipment failure) or a major disruption (such as fire, an extended power failure or a natural disaster). Once the business priorities are set out in the business continuity plan, IT continuity planning then occurs to identify where and how the supporting IT applications and systems would be vulnerable to damage or failure. The result is development of an IT continuity plan that specifies all the IT exposures to risk and sets out the solutions to deal with those risks. The disaster recovery plan, a subset of the IT continuity plan, prepares for major events that result in the relocation of IT processing for an extended period.

Source: Prepared by Office of the Auditor General of British Columbia

Why is IT continuity planning important?

One of the top causes of business disaster in public and private organizations is IT failure. Some researchers have estimated that of companies that suffer a major loss of computerized records, 43% will never reopen, 51% will close within two years, and only 6% will survive in the longer term (Cummings, Haag and McCubbrey 2005).

In British Columbia, the province's reliance on IT has intensified over the last decade with growing promotion of citizen-centred service delivery through e-business and greater sharing of information and systems between government and the broader public sector. The increased complexity of the information systems supporting critical programs has added to our dependency on IT to keep programs running. Today, more than ever before, information and technology management has become a vital component in the delivery of government programs.

International events such as Hurricane Katrina, the September 2001 terrorist attacks on the World Trade Center, the tsunami in Indonesia, and even the pandemic threat of the swine flu are reminders to government and the public that we need to plan how to deal with the effects of disaster and pandemic hazards so we can carry on. The recent earthquakes in Haiti and Chile are further reminders of the large earthquake event predicted for the Vancouver Island and Lower Mainland regions of British Columbia.

For all these reasons, proper IT continuity planning is necessary so that the impact on government programs from a disruption to the operation of business applications and supporting IT systems can be minimized.

What has the provincial government done to support IT continuity planning?

Without policies and procedures in place to support the effort, a structured process for the recovery of business systems and applications after a disaster can fail.

The provincial government established a formal, overall business continuity management program in 1996 when the Emergency Program Act was passed. Under this Act, each Minister must prepare emergency plans for responding to and recovering from a range of emergencies and disasters.

In addition, under the Emergency Program Management Regulation, each minister is responsible to "set out in business continuation plans and procedures, the manner in which and the means by which that minister will continue to provide essential services despite an emergency or disaster." These ministry business continuity management programs provide the foundation for government's overall approach to business continuity planning.

One of government's initial steps in preparing for possible disruption of services was to identify its "mission-critical" business functions, along with the IT applications and supporting systems used to deliver services related to those functions. Emergency Management BC compiled the government-wide ranking of business functions that, in the end, identified 49 as being program mission-critical and 22 as support mission-critical. Failure to recover these functions on a timely basis could result in loss of life, impaired public safety, or personal and financial hardship for citizens in British Columbia.

All of these critical programs and supports rely heavily on the continuous operation of computer applications and supporting systems to provide ministries with the information they need to make decisions, manage resources and deliver services. Protecting this information from deliberate or accidental destruction is therefore imperative.

Responsibilities for continuity planning have been assigned

Government's Core Policy and Procedures Manual and related government guidance have established responsibilities for continuity planning as follows:

- The Inter-Agency Emergency Preparedness Council (IEPC), made up of executive-level representatives from ministries and other public sector agencies, recommends to government coordinated response and recovery measures for the Province of BC.

- Emergency Management BC supports IEPC in developing and promoting policies and procedures for government wide response and recovery. It advises ministries on planning, developing, implementing and monitoring business continuity and recovery activities. Through the business continuity management program, Emergency Management BC provides essential reference information for ministries that are developing a business continuity management program.

- The cross-government BCMP (business continuity management program) Advisory Committee promotes, supports and improves the development of and adherence to standards and best practices for business continuity across government. The Committee, through its Chairperson, reports to the Deputy Ministry for Emergency Management BC.

- Ministries develop plans that include documented recovery strategies, procedures and current lists of key resources required for the recovery and resumption of essential services. Resources include personnel, facilities, critical infrastructure and assets, information, materials and office equipment, IT assets and communications. They must:

  - perform an annual strategic risk analysis of business objectives to identify business, program and operational risks that could be affected by a business interruption;

  - complete a comprehensive ministry-wide business impact analysis annually – and whenever significant program changes occur – to identify and develop strategies to reduce the likelihood and consequence of a business interruption;

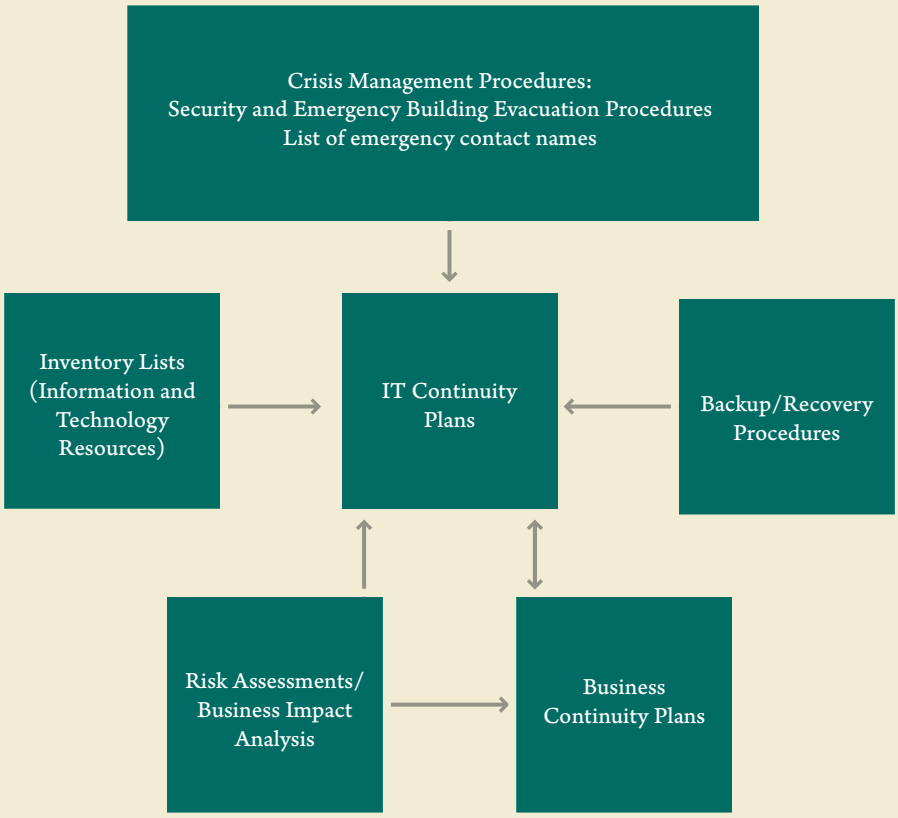
- identify internal and external dependencies involved in delivering government services, and develop mutually supportive continuity strategies; and

- exercise and update business continuity plans at least once a year, or as deemed necessary by the ministry's executive.

Exhibit 1 shows the relationship between IT continuity plans and the other documented procedures, plans, and assessments.

- Ministries must ensure their third-party service providers of supporting technology are held accountable for their contribution to recovery plans. Ministries should also work with service providers to develop and test business continuity and disaster recovery plans.

Exhibit 1: The relationship between IT continuity plans and associated documents required for business process recovery in British Columbia



Source: Adapted from the provincial government's MVS Disaster Recovery Plan

PURPOSE AND SCOPE OF THE AUDIT

The purpose of our audit was to assess whether the provincial government has adequate processes in place to ensure that, in the event of an emergency or disaster, all the IT applications and supporting systems and services required to deliver government's mission-critical business functions will continue to operate.

We selected sample mission-critical business functions from the government-wide ranking. These are shown in table 2.

The audit focused on IT continuity plans and related IT recovery exercises for the computer applications and supporting systems that these functions depend on. We also assessed how well each IT continuity plan aligns with ministry and government business continuity plans, and with government policies, procedures and regulations that relate to maintaining continuous IT services.

For each critical business function in our sample, we reviewed the development, maintenance and testing of the IT continuity plan and the ability for interim IT services and restoration to be provided. IT continuity plans were made up of ministry business continuation plans, a ministry plan for participation in the cross-government IT recovery exercise, documents collectively referred to as disaster recovery plans, and disaster recovery plans and business continuity plans of shared systems and services.

Our audit followed Canadian generally accepted auditing standards recommended by the Canadian Institute of Chartered Accountants. The audit procedures performed were based on the *IT Continuity Planning Audit/Assurance Program* developed by the Information Systems Audit and Control Association (ISACA).

Table 2: Mission-critical business functions from the governement-wide ranking

Business function	Provided by
Government-wide support systems and services	
Provision of the following shared systems and services: • *the UNIX/Linux, Windows, OpenVMS, MVS operating systems* • *network services, directories and authentication services (that manages govern ment userids and authentication), electronic messaging services (that manages government email), and IT security operations*	*Shared Services BC in the Ministry of Citizens' Services*
Program specific	
Coordination of ambulance and paramedic responses to emergency situations like 911 calls and air evacuations for movement of patients	*Vancouver Call Centre, part of BC Ambulance Service in the Ministry of Health Services*
Provision of case work and delivery of service, including contracts, placements, and payments for residential resources	*Children and Family Services in the Ministry of Children and Family Development*
Provision of payroll and human resource services to over 30,000 government employees at locations throughout the province	*Provincial Human Resources Management Systems (HRMS) Partnership Office at Shared Services BC in the Ministry of Citizens' Services*

WHAT WE FOUND

We looked at 22 controls in all and assessed, for each audit client in our sample, whether the procedures were in place and how effective they were. Our findings, by audit client, are summarized in table 3.

Following are detailed findings about how effectively the provincial government is managing IT continuity planning, organized first in regard to government as a whole and then by the four individual clients we included in our sample: Shared Services BC, BC Ambulance Service, Children and Family Services, and Provincial HRMS Partnership Office.

Table 3: Number of controls assessed for each audit client

Audit Client (number of samples)	Number of controls assessed as:		
	Adequate	*In place but needs improvement*	*Inadequate*
Shared Service BC (8)	*4*	*10*	*8**
BC Ambulance Service (1)	*12*	*4*	*6*
Children and Family Services (1)	*5*	*12*	*5*
Provincial HRMS Partnership Office at Shared Services BC (1)	*20*	*2*	*-*

**Two of these control procedures relate to cross-government responsibilities, not just those of Shared Services BC.*

GOVERNMENT-WIDE PERSPECTIVE

Government's Core Policy and Procedures Manual states that "good coordination and liaison involving inter-ministry activities and with service providers is critical to restoring business operations during and following an interruption." The policy goes on to add that "ministries must identify internal and external dependencies involved in the delivery of government services and develop mutually supportive business continuity strategies." As a result of our audit, we concluded that:

- It is likely that, in the event of a major disaster, not all applications supporting mission-critical business functions can be restored at the same time, as they will be competing for the same resources. Yet we found no overall government strategy for prioritizing recovery of mission-critical applications.

- The list of mission-critical business functions across government shows their necessary recovery times, which range from 3 to 48 hours. Many of these business functions use applications that run on the operating environments and other shared systems provided by Shared Services BC, through third-party service providers.

Shared Services BC provides two types of IT services:

- *Services based on common assets* – Resources are pooled and offered to ministries at a set service level. Examples include the MVS and Open VMS operating infrastructures, data backup and shared databases.

  IT continuity planning is designed and executed by Shared Services BC and included in the service price. An alternative recovery site and operating platform is provided. The recovery time objective for each operating platform is set – for OpenVMS and MVS at 72 hours. Ministries are invited to participate in recovery exercises, recovering their program applications and data after the operating infrastructure has been recovered.

- *Services based on dedicated assets* – Resources are dedicated to individual ministry programs and managed to predefined service levels. The program area can select the services and service levels required. Examples include the UNIX/Linux and Windows operating infrastructures.

  Ministries are responsible for the design and execution of IT continuity planning. An alternative recovery site and operating platform is not included in the base-level service, but the option is available through explicit service agreements.

It is each ministry's responsibility to ensure necessary arrangements are in place to meet its recovery time objectives. This can be done with the ministry stipulating that requirement in a memorandum of understanding or service-level or explicit agreement.

It is also each ministry's responsibility to work with service providers to develop business continuity and disaster recovery plans. As we were told no specific agreements for continuity purposes have been made by ministries with the third-party provider of UNIX/Linux and Windows operating infrastructures, there is a risk that some mission-critical business functions will not be restored within their established recovery timelines.

SHARED SERVICES AND SYSTEMS PROVIDED BY SHARED SERVICES BC

Most of government's mission-critical applications run on shared systems and use shared services, making the continuous operation of these shared systems and services vital to the functioning of government programs. These applications rely on the availability of servers and related operating systems, and also on the government's voice and data networks, communication software and directories, authentication and security infrastructure.

To assess whether adequate processes are in place to ensure shared services and systems can be restored and ready for service within required timelines, we reviewed the following business functions in Shared Services BC:

- IDIR directory (the BC Government Employee userid directory) and authentication services are required to access internal government computer resources and e-services. This access is available to users who are within government and the broader public sector.

- Integrated messaging and collaboration applications supply a scalable platform on which to deliver communication tools such as e-mail, calendaring, contact, task management, instant messaging and desktop video conferencing.

- Developing, implementing and managing a comprehensive security infrastructure is the responsibility of IT Security Operations and ensures the confidentiality, integrity and availability of the government IT infrastructure and the data that resides within and transits that infrastructure.

- Operating Systems (MVS, OpenVMS, UNIX/Linux and Windows) are delivered through the following alternative service delivery contracts that are managed by Hosting Services:

  - IBM provides MVS hosting services until January 30, 2011, when it is outsourced to EDS Advance Solutions (EAS), now called Advanced Solutions An HP Company. This service is currently subcontracted to TELUS. The MVS (also known as z/OS) platform accommodates some of the provincial government's larger computing applications.

  - EAS provides UNIX/Linux, Windows and OpenVMS hosting services as of March 30, 2009. The Unix/Linux or Windows hosting service provides a dedicated operating system image on which customers can build and run their business applications. The OpenVMS Service provides a shared platform for customers to develop, manage and run their own applications in a scalable environment with operating system and storage subsystem support.

- Network services has approximately 50 contracts in place with various data network and voice service providers. TELUS is the major provider of the infrastructure for the delivery of data and voice services to government.

Generally, Shared Services BC has plans and processes in place to provide interim IT services and subsequent restoration of services. However, improvements are needed in certain areas of the IT continuity planning process to ensure that these critical systems and others dependent on them can survive all levels of disaster.

Identifying risks and prioritizing recovery of services

- Shared Services BC has used risk assessment and business impact analysis methods to establish business interruption exposures, their probability and impact, and remediation alternatives. However, the risk assessment and business impact analysis completed in 2003/04 have never been updated even though several reorganizations have occurred since then and a major alternative service delivery contract negotiated.

- Essential business processes, the recovery time objectives, resource requirements, interdependencies and business unit contact lists have all been identified as part of the risk analysis that Shared Services BC did in developing its business continuity plans. Business continuity plans are created for each business unit, and each business unit is responsible for maintaining its continuity plan.

Developing IT continuity plans

- Shared Services BC has a business continuity management program in place. The program is administered by the IT Security Operations group. The sample business continuity plans were signed off by the Assistant Deputy Minister.

- Shared Services BC has not prepared an overall budget for business continuity planning. Doing so would ensure that adequate resources are assigned to the business continuity planning process, as well as emphasizing the importance of this function.

- Disaster recovery plans have been prepared for the MVS, OpenVMS, and systems used in providing directories, authentication and electronic messaging services (Windows 2003 Active Directory, Government Telephone Directory, Web Access Management and Exchange 2003 platforms). These services are based on common assets, and IT continuity planning is designed and executed by Shared Services BC.

- Formal disaster recovery plans have not been prepared for various network infrastructures and it is unclear whether they exist for the Windows and UNIX/Linux platforms. This creates a risk that these infrastructures may not be restored in a timely manner if a major disaster occurred. Ministries are responsible for the design and execution of IT continuity planning for their mission-critical programs and applications. This is discussed above under "Government-wide perspective."

- Service delivery and service-level agreements are not in place for all the sample applications we tested. These agreements would identify the business continuity requirements of customers, and clearly define the responsibilities between Shared Services BC and its customers. This is also discussed above under "Government-wide perspective."

Ensuring IT recovery plans are appropriate and complete

- Staff responsibilities and notification procedures are documented in the business continuity plans and in the MVS, OpenVMS and Exchange 2003 disaster recovery plans. However, access procedures are not documented in business continuity plans and substitution procedures are not in place in the business continuity and disaster recovery plans.

- Data recovery and restore responsibilities have been established for hosting services and data recovery procedures for key applications at Messaging and Collaboration Services, Network Services and IT Security Operations.

- Recovery sites and backup facilities are mostly located in Victoria and Vancouver, which is within the same geographical area as the primary data centre and – like the latter – lying within British Columbia's most active earthquake zone. This poses a threat to all facilities in the event of a major quake. With the new alternative service provider agreement, there is a five year process to relocate the current Victoria data centre to a Calgary and Kamloops location, both being outside of the geographic earthquake area. However, anything could happen between now and the date the data centre moves to Calgary and Kamloops, which could adversely impact the Victoria data centre facility.

- Contracts related to the audit sample of shared systems and services include business continuity and disaster recovery requirements. However, we found that these requirements are inconsistent and we were told that some of the other major infrastructure contracts of Shared Services BC predate the formal business continuity plan policy requirement. This could put the timely recovery of critical processes at risk if a disaster were to occur.

Testing IT continuity plans regularly

- Business continuity plans have been updated and tabletop and partial functional exercises are conducted annually. However, according to government policy and guide, more than tabletop and partial functional exercises should be performed to confirm the plan's effectiveness. There is also a need to increase the use of unannounced events or unplanned situations as business continuity planning processes mature.

- The disaster recovery plan for OpenVMS was tested during 2009, but not the MVS. Planned testing of government email is not performed; however, restores are done throughout the year based on requests from customers. None of the other disaster recovery plans of Shared Services BC have yet been tested.

- The tests performed in 2008 for the MVS and OpenVMS disaster recovery plans were documented. However, the documentation for tests performed for the business continuity plan does not include detailed action plans, comparisons of performance results against test criteria (such as recovery time objectives and recovery point objectives), and tracking of the resolution of issues and lessons learned.

Keeping IT continuity plans current

- Except for the MVS, none of the other disaster recovery plans in Shared Services BC has maintenance and revision procedures. Also, the recovery plans for Windows 2003 Active Directory, Government Telephone Directory, Web Access Management, and Exchange 2003 do not explicitly detail who is responsible for maintaining the plans.

- It was not clear to us how many of Shared Services BC's continuity plans are reviewed and updated as part of application and systems changes or upgrades.

BC AMBULANCE SERVICE, VANCOUVER CALL CENTRE

Our sample included a mission-critical business function in BC Ambulance Service (BCAS). According to statistics on its website, BCAS has 187 stations, 470 active ambulances and 3 flight centres across the province. The program schedules and dispatches over 525,000 ambulance calls and over 8,500 air ambulance calls a year.

Ambulance services are scheduled and dispatched from four call centres covering four separate regions in the province: the Lower Mainland (Vancouver), Vancouver Island (Victoria), Interior (Kamloops) and Northern (Prince George). The provincial air ambulance dispatch centre is in Victoria.

The main IT applications used by call centres to support the coordination of ambulance and paramedic responses to emergencies include:

- a system used by call centres to automate their dispatch function, which includes receiving requests for service, dispatching ambulances and air ambulances, monitoring and progressing service delivery, and managing ambulance units; and

- a system used to receive and store patient care records and dispatch records and assign a bill type

Call centres also rely heavily on the communication systems and related services provided by TELUS and Shared Services BC to support the coordination and response to emergency calls.

Our audit focused on the Vancouver call centre.

Identifying risks and prioritizing recovery of services

- BCAS has identified mission-critical functions and the IT applications and supporting systems required to sustain them.

- BCAS has completed the initial phase of a business impact analysis. To be in compliance with government policy, the organization should be completing a comprehensive business impact analysis annually, as well as when significant program changes occur.

Developing IT continuity plans

- Business continuity planning is administered by the Information Management and the Corporate Policy and Planning departments within BCAS. Business continuity plans are created for each individual program area and the program area is responsible for maintaining and reporting on its continuity planning. We found that the business continuity plan, Operations for the Lower Mainland, details essential business processes, the recovery time objectives, resource requirements, interdependencies and business unit contact lists.

- BCAS does not have a formal IT continuity plan that aligns with and supports the business continuity plan. Rather there are several individual documents that are collectively referred to as a disaster recovery plan. As there is no overall plan that refers to these documents, we think this could result in certain risks not being considered or adequately planned for.

- BCAS has not prepared an annual budget for testing and updating continuity plans and their components. Putting a budget in place would ensure that adequate resources are assigned to the business continuity process, as well as emphasizing the importance of this function.

Ensuring IT recovery plans are appropriate and complete

- The Lower Mainland call centre works closely with the primary 911 centre for police in the Greater Vancouver area. Each centre provides the other with some backup capacities and an agreement is in place for the 911 centre to act as a "hot site" for the Lower Mainland dispatch centre. However, we noted that this alternative (or "failover") site is only several kilometres

from the BCAS call centre. With these centres being so close to each other, there is a risk that both facilities could be destroyed if a major disaster occurred.

- Data recovery procedures have been established and tested to ensure availability of data.

- The communications components (data and voice) necessary to provide network access to the computing facilities is the responsibility of Shared Services BC and TELUS. Again, recovery relies on these networks being available, which reinforces the necessity for explicit service agreements. This is discussed above under "Government-wide perspective."

Testing IT continuity plans regularly

- BCAS performed no situation drills – tests in which resources are purposely not available or the circumstances of the tests are modified unannounced to verify the recovery team's ability to adapt to unplanned situations.

- Results of recovery plan tests are analyzed and corrections implemented as necessary. However, we found that the results of tests and corrections made are not being formally communicated to the appropriate level of senior management for their review and approval.

Keeping IT continuity plans current

- The business continuity plan was dated March 2007, but still in draft at the time of our field work. Sections of this plan require updating and BCAS should ensure that its recovery plans are updated annually.

CHILDREN AND FAMILY SERVICES

We selected a mission-critical business function, Children and Family Services, in the Ministry of Children and Family Development. The main computer application supporting this business function is a management information system running on a MVS operating system provided through a service delivery arrangement with Shared Services BC. This system is also used by the Ministry of Housing and Social Development. The IT services are shared between the two ministries.

Four components of the management information system are classified as mission-critical:

- *Intake and Child Services* – provides support for case work and delivery of service, allowing case workers to maintain an electronic record of all child protection reports and requests for support;

- *Resource and Payment System* – supports all stages of the resource management cycle including resource set-up, contracts, placements and payments for residential resources;

- *Central Registry* – a provincially accessible database that contains unique identifying records for most of the past and present clients of the ministry; and

- *Reportable Circumstances* – provides a standard method for ministry staff to follow in dealing with reportable circumstances in order to create a document with all pertinent information.

Failure to recover these system components on a timely basis could impact the public by resulting in loss of life, impaired public safety or personal hardship.

Identifying risks and prioritizing recovery of services

- The ministry has done some risk analysis, listing business processes and identifying those considered mission-critical. Interruption scenarios have also been identified. However, a documented risk assessment and business impact analysis is not being carried out annually, as required by government policy.

- Many of the ministry's mission-critical business processes have recovery time objectives of less than 8 hours. That might be achievable in a localized disaster, but not a major disaster that would force the operating system to be brought up at the alternative site. The target for bringing up this operating infrastructure is 72 hours.

- The ministry business continuity plan does not cover restoration of ministry printers or address recovery priority of mission-critical applications.

Developing IT continuity plans

- The business continuity plan we sampled is prepared and maintained by a branch of the Office of the Ministry Chief Information Officer. It is based on an "all-hazards" approach, where the magnitude and the reason for the interruption are not defined. Planned actions are written to be adaptable.

- The ministry has incorporated certain components of an IT continuity plan – such as recovery of the applications and the operating infrastructure – in the business continuity plan. The ministry also has a test plan for its participation in the MVS recovery exercise coordinated by Shared Services BC. This plan has detailed recovery steps, including database restore procedures.

- The ministry does not have a separate identifiable budget set up for testing and updating continuity plans and their components. Having one can be an effective way to ensure a financial commitment is maintained.

Ensuring IT recovery plans are appropriate and complete

- Application maintenance and development services relating to the management information system were awarded to a third-party provider in May 2004. The disaster recovery plan of the third party was last updated in January 2005. As test documentation was not available, we could not evaluate its effectiveness. Third-party continuity plans should subscribe to the same policies, standards and guidelines as the government's continuity plan does with regard to frequency of update and exercise.

- The communications components (data and voice network) are not included in the ministry's continuity planning as they are considered to be the responsibility of Shared Services BC. Recovery of the management information system relies on these networks being available, reinforcing the need for service delivery or service-level agreements. This is discussed above under "Government-wide perspective."

- Alternative cheque-printing arrangements for the ministry are located in the same geographical area and both sites lie within British Columbia's main earthquake zone.

  The impact of a potential disruption to cheque payments is lessened given the ability to issue manual cheques in field offices located elsewhere in the province.

- No alternative site location is noted for staff to continue carrying on critical business functions if their main location is damaged or destroyed.

Testing IT continuity plans regularly

- The ministry's business continuity plan is not being tested annually.

- The ministry participates in an annual IT recovery exercise that Shared Services BC coordinates through a third-party service provider. During this exercise, the third-party provider coordinates the recovery of the MVS operating system platform and the recovery of various systems to the point where Shared Services BC customers – such as the ministry – can restore their own user data and then validate their application systems.

- To speed up the exercise timelines, a large component of pre-exercise planning is conducted over a four-month period. The last exercises were conducted in December of 2008 when recovery of the application was tested. The third-party vendor providing application maintenance and development services for the application was involved with the recovery. Exercise issues were followed up and resolved. These tests require significant pre-planning and therefore the ministry does not use situation drills – tests in which resources are purposely not available or the circumstances of the tests are modified unannounced to verify the recovery team's ability to adapt to unplanned situations.

Keeping IT continuity plans current

- The ministry's business continuity plan is not being updated annually.

- Neither the system development methodology nor the system enhancement process includes steps to ensure the continuity plans are being updated

GOVERNMENT PAYROLL AND HUMAN RESOURCE FUNCTION

Our sample included the government payroll and human resource function, which is the responsibility of the Provincial HRMS Partnership Office, Shared Services BC, in the Ministry of Citizens' Services. These services are delivered to over 30,000 employees in more than 40 government ministries, agencies and Crown corporations at various locations across the province.

The payroll function was outsourced to a third-party service provider in November 2004. Management of the contract is the responsibility of the Provincial HRMS Partnership Office. Payroll processing is performed at the service provider's processing centre located in Victoria. The dedicated servers for the province are hosted at the service provider's data centre, also in Victoria, and the service provider's personnel provide server and database administration support.

The main applications used are the corporate human resource information and payroll system and the automated time-capture application.

Overall, we found that the service provider has a well-established business continuity and disaster recovery planning process in place.

Identifying risks and prioritizing recovery of services

- The service provider conducted an informal business impact assessment that included key objectives such as identifying key business functions, understanding the risks, and recommending strategies to mitigate those risks. This approach appears reasonable to us as the contract clearly identified the service provider's responsibilities with regard to business continuity and disaster recovery planning. Specifically, the contract identified the critical business functions and the associated recovery timeframe necessary to guide the service provider's recovery strategy and plans.

- Although recovery time objectives have been established, recovery point objectives appear not to have been. However, based on documentation we reviewed, we concluded that minimal data would be lost given the "near real-time" copies of critical databases that are maintained at the backup data centre.

Developing IT continuity plans

- Continuity and disaster recovery roles and responsibilities are established in the Provincial HRMS Partnership Office business continuity plan and the service provider business continuity and disaster recovery plans.

- The Province is sending the service provider a copy of the Provincial HRMS Partnership Office's business continuity plan at least annually and when it is updated. This helps ensure that it and the IT continuity plans of the service provider will be consistent with each other.

Ensuring IT recovery plans are appropriate and complete

- Under normal operations, the government's network is used for communication. If there was a disaster creating a connectivity problem, the service provider could provide support.

- The agreement with the service provider has a section on business continuity and disaster recovery planning. Under the agreement, the business continuity plan must subscribe to the same policies, standards, guidelines and procedures as are in the government's business continuity plan. The service provider has provided the provincial government with a copy of the plan.

- The service provider's business continuity plan is detailed and includes information on alternative facilities and staff responsibilities. Critical applications and supporting platforms have been identified, and the required software and data are available for interim processing and restoration.

- The agreement with the service provider states that the provider will supply the Province with updated contact lists. We verified that this is being done.

- Although under the agreement, the service provider has assumed all responsibility for the provision of disaster recovery and business continuity services, the Province remains responsible for monitoring the service provider's compliance with requirements outlined in the agreement. This compliance is evident in documentation sent to the Province by the service provider and in the section in the annual Independent Service Auditors Report relating to business disaster and continuity processes.

Testing IT continuity plans regularly

- The IT continuity plan is being tested annually in accordance with the action plan.

- Tests do not include situation drills – tests in which resources are purposely not available or the circumstances of the tests are modified unannounced to verify the recovery team's ability to adapt to unplanned situations. Plan testing should also include verification that the tests are completed within the recovery time objectives established in the business continuity plan.

Keeping IT continuity plans current

- The service provider's business continuity plan, which includes disaster recovery planning, was updated as of May 2009 and the updates sent to the Province.

APPENDIX

GLOSSARY

Alternative service delivery (ASD) – The primary focus is to provide cost-effective and efficient delivery of services through innovative partnering with the private sector. Objectives include:

- Maintaining or enhancing service levels
- Allowing government to focus its resources on more strategic areas
- Reducing costs, increasing revenue, or maximizing cost avoidance
- Transferring operational risk to service providers
- Harnessing the combined creativity of the private and public sectors
- Supporting general economic development and growth *(Source: www.lcs.gov.bc.ca/asd/)*

Application – a program or group of programs designed for end users. Software can be divided into two general classes: *systems software and applications software.* Systems software consists of low-level programs that interact with the computer at a very basic level. This includes operations systems, compilers, and utilities for managing computer resources. In contrast, applications software (also called *end-user programs*) includes database programs, word processors, and spreadsheets. Figuratively speaking, applications software sits on top of systems software because it is unable to run without the operating system and system utilities. (*Source: www.webopedia.com*)

Business continuity – a form of risk management activated when standard operational procedures and responses are overwhelmed by an interruption or event. While Emergency Response focuses on event containment and consequence management, Business Continuity focuses on ensuring that critical services are resumed until a return to normal business operations is possible. (*Source: BC Provincial Government Core Policy and Procedures Manual*)

Business continuity management program (BCMP) – includes planning, developing, implementing and monitoring business continuity and recovery activities in all ministries and agencies. (*Source: BC Provincial Government Core Policy and Procedures Manual*)

Business continuity plan (BCP) – an enterprise-wide group of processes and instructions to ensure the continuity of business processes in the event of an interruption. The BCP focuses on sustaining an organization's business functions during and after a disruption. A BCP may be written for a specific business process or may address all key business processes. IT systems are considered in the BCP in terms of their support to the business processes. In some cases, the BCP may not address long-term recovery of processes and return to normal operations, solely covering interim business continuity requirements. A disaster recovery plan, business resumption plan, and occupant emergency plan may be appended to the BCP. (*Source: NIST IT Contingency Guide*)

Business continuity planning – the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. (*Source: NIST IT Contingency Guide*)

Business impact analysis (BIA) – analysis of an IT system's requirements, processes, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption. (*Source: NIST IT Contingency Guide*)

APPENDIX

Disaster recovery plan (DRP) – applies to major, usually catastrophic, events that deny access to the normal facility for an extended period. Frequently, DRP refers to an IT-focused plan designed to restore operability of the target system, application, or computer facility at an alternative site after an emergency. The DRP scope may overlap that of an IT contingency plan; however, the DRP is narrower in scope and does not address minor disruptions that do not require relocation. Dependent on the organization's needs, several DRPs may be appended to the BCP. (*Source: NIST IT Contingency Guide*)

Drill exercise – exercise that tests and develops skills in a single-focus response procedure. A drill usually involves the activation of a single procedure (e.g., communications through the use of call-out lists), that would be involved in an actual disaster or major emergency. (*Source: BC Provincial Government Business Continuity Management Guidelines*)

Full-scale exercise – exercise intended to evaluate the capability of the organization to respond to and recover from a disaster. An exercise of this type will require a major commitment and personnel and resources. This type of exercise is not normally done but is highly effective. (*Source: BC Provincial Government Business Continuity Management Guidelines*)

Functional exercise – exercise used to evaluate the capability of one or more functions or complex activities. There is full simulation using messages that are delivered by means of phone and/or radio. Stress is introduced at this level because of the number of messages and the coordination and decision-making that are required to respond to the simulation. This scenario is more realistic but is a controlled situation. The time pressures are presented through simulation of specific activities. (*Source: BC Provincial Government Business Continuity Management Guidelines*)

Hot site – a fully operational off-site data processing facility equipped with hardware and system software to be used in the event of a disaster. (*Source: NIST IT Contingency Guide*)

Information system – A system (including people, machines, methods of organization, and procedures) which provides input, storage, processing, communications, output and control functions in relation to information and data. Normally used to describe computerized systems, including data processing facilities, database administration, hardware and software which contain machine-readable records. (*Source: BC Provincial Government Core Policy and Procedures Manual*)

Information technology (IT) – The common term for the entire spectrum of technologies for information processing, including software, hardware, communications technologies and related services. (*Source: BC Provincial Government Core Policy and Procedures Manual*)

Information and technology resources – Information and communications technologies, including data, information systems, network services (e.g. web services; messaging services); computers (e.g. hardware, software); telecommunications networks, and associated assets (e.g. telephones, facsimiles, cell phones, laptops, personal digital assistants). (*Source: BC Provincial Government Core Policy and Procedures Manual*)

IT continuity plan (ITCP) – addresses the IT exposures and solutions based on the priorities and framework of the business continuity plan. (*Source: ISACA IT Continuity Management Audit Program*)

IT continuity planning – the process that ensures continuous operations of business applications and supporting IT systems; a subset of business continuity planning. (*Source: ISACA IT Continuity Management Audit Program*)

Linux – a freely-distributable open source operating system that runs on a number of hardware platforms. The Linux kernel was developed mainly by Linus Torvalds and it is based on UNIX. Because it's free, and because it runs on many platforms, including PCs and Macintoshes, Linux has become an extremely popular alternative to proprietary operating systems. (*Source: www.webopedia.com*)

MVS – short for Multiple Virtual Storage, the operating system for older IBM mainframes. MVS was first introduced in 1974 and continues to be used, though it has been largely superseded by IBM's newer operating system, OS/390. IBM's mainframe operating system is now called z/OS. (*Source: www.webopedia.com*)

APPENDIX

OpenVMS – VMS (Virtual Memory System) is a multi-user, multitasking, virtual memory operating system that runs on DEC's (Digital Equipment Corporation) VAX and Alpha lines of minicomputers and workstations. It was first introduced in 1979 and has undergone many changes over the years. DEC now refers to it as OpenVMS. (*Source: www.webopedia.com*)

Recovery point objective (RPO) – the earliest point in time at which it is acceptable to recover the data. It is based on what an organization agrees is an acceptable or permissible amount of data loss during a disruption. (*Source: ISACA Glossary of Terms*)

Recovery time objective (RTO) – the earliest point in time at which business operations must resume after disaster. It is determined based on the acceptable extent of down time in the case of a disruption of operations. (*Source: ISACA Information Systems Control Journal, Volume 1, 2005, Auditing Business Continuity*)

Tabletop exercise – A walk-through exercise where team members meet as a group in a conference room setting and verbally role-play their positions through a given scenario. Tabletop exercise does not focus on stress, time, pressures, or simulations of actual events, but on problem solving. Exercise results identify issues, gaps and limitations and lessons learned are used to improve and update plans. (*Source: BC Provincial Government Business Continuity Management Guidelines*)

UNIX – a popular multi-user, multitasking operating system developed at Bell Labs in the early 1970s. Created by just a handful of programmers, UNIX was designed to be a small, flexible system used exclusively by programmers. Bell Labs distributed the operating system in its source language form, so anyone who obtained a copy could modify and customize it for his own purposes. By the end of the 1970s, dozens of different versions of UNIX were running at various sites. (*Source: www.webopedia.com*)

Windows – short for Microsoft Windows, a family of operating systems for personal computers. Windows provides a graphical user interface (GUI), virtual memory management, multitasking, and support for many peripheral devices. (*Source: www.webopedia.com*)