PART 6

INFORMATION TECHNOLOGY

VERSION 1

TABLE OF CONTENTS

SECTION TABLE OF CONTENTS

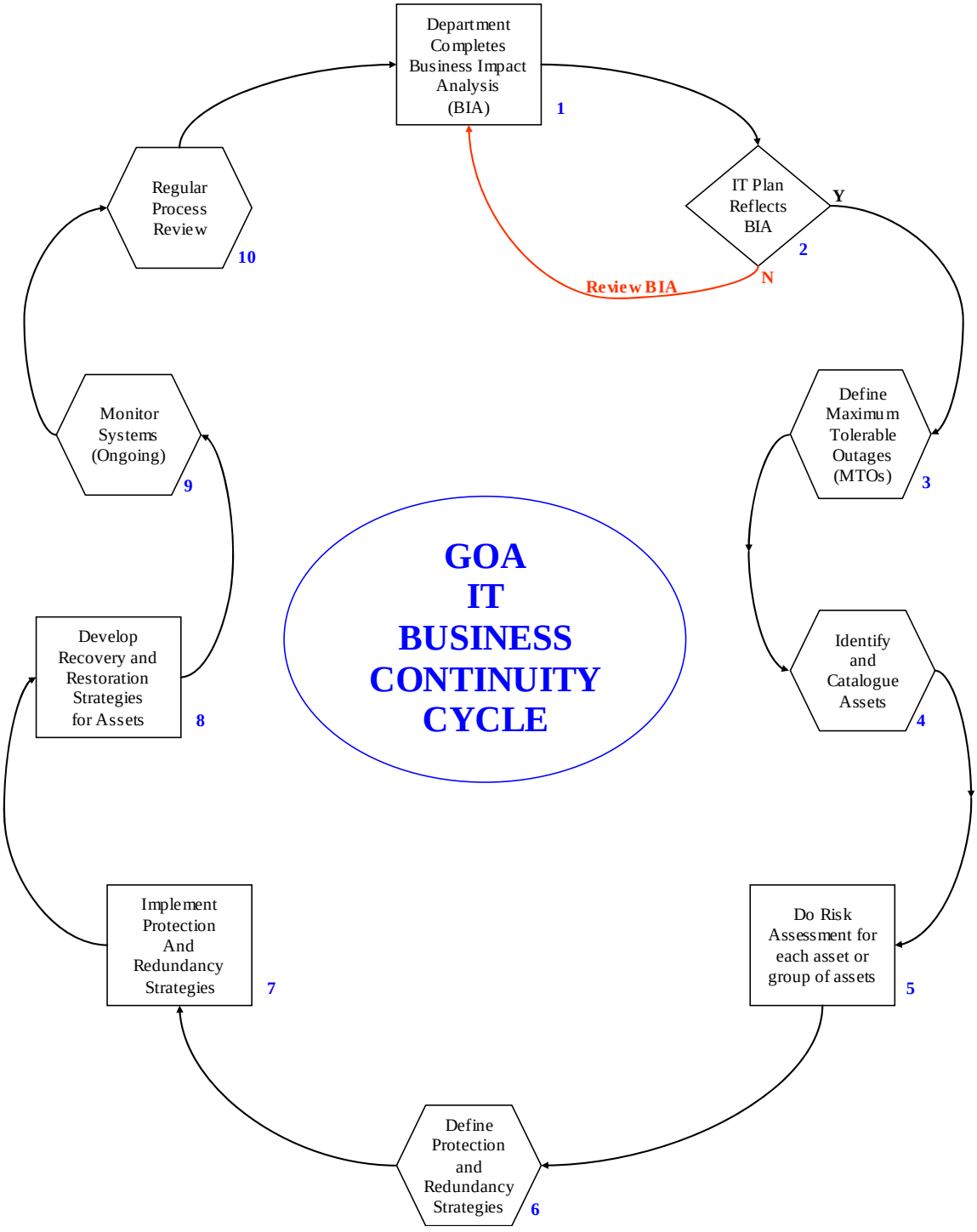
CONTRIBUTORS

The Alberta Emergency Management Agency would like to thank the following Information Technology professionals who have contributed substantially to the development of this Business Continuity Information Technology Guide through content contribution and peer review:

- James Berge – Manager, Business Services, Strategic Corporate Services, Alberta Emergency Management Agency
- David Cunningham - Director, Information Technology Strategic Planning, Alberta Energy
- Deborah Harrop - Senior Manager, IT Infrastructure Information Management, Workers Compensation Board of Alberta
- Harry Henshaw - Research Officer, Strategic Technology Planning, Alberta Advanced Education and Technology
- Herb Presley - A/Manager of Business Continuity, Alberta Emergency Management Agency (primary content author)

1. INTRODUCTION

1.1 IT BUSINESS CONTINUITY CYCLE



A detailed description of each element is provided.

1.2 GOA IT BUSINESS CONTINUITY CYCLE ELEMENTS

1. *Department Completes Business Impact Analysis (BIA)* - See Paragraph 2.1 of the IT Business Continuity Guide. Each department of the GoA should complete a BIA that defines their essential services. The business continuity programs of IT systems should be designed to support the department BIA.
2. *IT Plan Reflects BIA* - See Paragraph 2.1.1 of the IT Business Continuity Guide. This is a decision point. If the IT processes reflect the departmental BIA (Y=Yes) then proceed to the next step. If the IT processes do not reflect the departmental BIA (N=No) then go back to step 1 and ensure that IT processes fall in line with the BIA.
3. *Define Maximum Tolerable Outages (MTO's)* - See Paragraph 2.1.4 of the IT Business Continuity Guide. Define the maximum time that an essential service is allowed to be not available, in particular if the MTO has a shorter period than the 24 hour limit outlined for a "critical" essential service.
4. *Identify and Catalogue Assets* - See Paragraph 2.7 of the IT Business Continuity Guide. A parallel must be drawn between the essential services supported in the BIA and the IT assets used to support each essential service.
5. *Do Risk Assessment for each asset or group of assets* - See Paragraph 2.2 of the IT Business Continuity Guide. Risk should be defined as not only the hazards that are present to the IT syststems but more importantly, the potential loss that is faced in the event of a system failure. A separate risk analysis will assist in determining the vulnerabilities of each IT asset.
6. *Define Protection and Redundancy Strategies* - See Paragraph 2.4 of the IT Business Continuity Guide. It is important to protect systems from failure rather than focussing on recovery from failure. Prevention strategies can be inexpensive and can mainly consist of practical and prudent practices.
7. *Implement Protection and Redundancy Strategies* - See Paragraph 2.4.1 of the IT Business Continuity Guide. One strategies are defined, they should be implemented, in particular if they involve prudent practices that must be learned and maintained.
8. *Develop Recovery and Restoration Strategies for Assets* - See Paragraph 2.5 of the IT Business Continuity Guide. Restoration and recovery strategies developed should be based on the results of the BIA, including the critical time frames and available alternative manual procedures in the event of an extended computer coverage.
9. *Monitor Systems (Ongoing)* - Often this is the most difficult part of the cycle. It should include a program of system testing and exercising of the BIA as outlined in Paragraph 2.9.5 of the IT Business Continuity Guide.
10. *Regular Process Review* - A review of the applicability of the IT Business Continuity Plan should be done at least annually in relation to support of the Departmental BIA. The GoA Business Continuity Cycle should start again at each annual review.

1.3 BACKGROUND

Departments of the Government of Alberta have a heavy operational dependency on Information Technology (IT), including Wide and Local Area Networks, Database Servers, Internet, Intranet and e-Mail. The potential loss of essential services to Albertans and operational control that may occur in the event of an interruption in information technology systems necessitate the preparation, implementation and maintenance of a comprehensive Information Technology Business Continuity Strategy.

Departments currently have and maintain a written Business Continuity Plan for maintenance of essential services that should include and provide information on Information Technology (IT) backup procedures and recovery procedures from system failure and breakdown.

As this guide is studied it is important to realize that Information Technology is a volatile, changing field. New IT assets are continually being developed to better serve the information needs of individuals, businesses, organizations and public bodies. Therefore in order for this guide to remain current on the Information Technology employed by departments of the GoA, it must always be considered a work in progress.

The guide suggests methods to assist departments of the GoA with both the Business Continuity of Information Technology and Disaster Recovery after system failure. Its key mission is to heighten awareness of the need for an IT Business Continuity Plan to be anchored to and support the department Business Continuity Plan.

1.4 PURPOSE

The purpose of this document is to guide Business Continuity Managers and their teams through the process of incorporating an IT Business Contuity Strategy as a component of their overall department Business Continuity Plan, preferably as a key annex. It is the intent that this component would provide for the continuity, protection, restoration and recovery of key data and systems.

The guide is not a plan, it is not a plan template, nor is it primarily designed to assist in the writing of a plan. It is designed assist in the establishment of good business continuity practices for GoA IT principals and, as such has been written in an instructive and suggestive tone. It's underlying theme is to help IT department staff and managers to integrate the main department BCP and overall GoA BCP planning in their system protection, security and restoration procedures and techniques.

There are two key principles that should guide a department in the development of an IT Business Continuity Strategy.

A. IT applications that support the essential services of the department should be given priority according to the criticality of the service.

B. Maintenance and prevention of IT systems failure provides a greater benefit to IT system continuity than restoration and recovery.

The IT Business Contuity Strategy process should include several major steps[1] which, when conducted, will ensure the completeness of the department's guide.

- ☐ The identification of systems and applications currently in use.
- ☐ Analysis of the business impact of information technology on essential services.
- ☐ Protection Strategies to minimize the impact of a disruption of services.
- ☐ Planning to meet critical recovery time frames.
- ☐ Determination of mitigation and recovery strategies.
- ☐ Documentation of the IT Business Continuity Team Organization.
- ☐ Documentation of the responsibilities of the IT Business Continuity Team.
- ☐ Development and documentation of emergency procedures.
- ☐ Develop and document training and maintenance procedures.

1.5 MISSION AND OBJECTIVES

The mission of an IT Business Contuity Strategy is to establish defined responsibilities, actions and procedures to protect and recover a GoA Department's essential information technology systems, including its communication and network environment in the event of an unexpected or unscheduled disruption.

Protection Strategies should address:

- Making certain that an overall development plan exists for the existing needs and the future growth of your department's information technology systems.
- Ensuring that changes and patches to your IT systems are compatible with its existing technology.
- Developing and maintaining a sound preventive maintenance program that allows for anticipation of equipment failures and deviations from unassailable operation.

[1] This standard checklist can be used to ensure no major steps are overlooked.

- Ensuring that cost effective options are available for alternate operation of system applications and hardware.
- A regular program of offsite data storage of sufficient frequency to ensure that lost data can be retrieved in a timely fashion.

The Recovery Plan should be structured to attain the following objectives:

- Recover the physical network and components within the critical time frames specified in the Department's Business Impact Analysis (BIA) framework specified in the Business Continuity Plan (BCP);
- Recover essential information technology applications and functions within the critical time frames specified in the department's BIA framework specified in the BCP; and
- Minimize the immediate and long term operational impact on department essential services and regular business.

1.6 SCOPE

The scope of a Business Continuity Information Technology Plan should afford protection and restoration to four major components of information technology.

1. Computers and computer network hardware.
2. Systems that support computers and networks (e.g.: electrical power systems).
3. Software applications that support the business services of a department (e.g.: word processing, spreadsheet, database and e-Mail applications).
4. Telecommunications systems that are managed by a department (e.g.: PBX systems that are not part of a vendor managed service).

1.7 AUTHORIZATION

A Business Continuity Information Technology Plan should exist as both an annex to the main Business Continuity Plan of the department and a stand alone document which focuses on the information technology services.

The Plan should be authorized and signed off in the following manner:

> *"The need for a Business Continuity Information Technology Plan has been recognized by the senior management of [name of department] for the protection, recovery and restoration of electronic applications and information that support this department's essential services and their delivery to Albertans. The following signatories hereby authorize the use of*

this plan in all circumstances that require the safeguarding of information technology."

It is suggested that a separate page at the beginning of the plan should contain this statement and be signed by the following and each signature dated:

- The most senior department official(s) responsible for information technology services;
- The line manager of the information technology section; and
- The most senior manager of the main vendor providing a major element of the information technology as a supplied service.

1.8 RESPONSIBILITY

The responsibility for the development, maintenance and updating of an Information Technology Business Continuity Plan should be assumed by a person or organization within the department that has the responsibility for day to day operation and maintenance of the computer or telecommunications systems. The end user communities of the systems are responsible to coordinate with the IT Business Continuity Plan manager for their business continuity information technology requirements.

In order to ensure that the management of the IT Business Continuity Plan receives adequate priority, it is important that the IT Business Continuity Plan Manager is at liberty to discuss issues relating to the IT Business Continuity Plan with the most senior management of the department at any time.

1.9 IT BUSINESS CONTINUITY PLAN ORGANIZATION

The formation of a team to monitor and update the IT Business Continuity Plan is important to its continued effectiveness.

1.9.1 TEAM MEMBERSHIP

Membership on the IT BCP team should consist of at least the persons filling the roles of[1]:

- Senior management of IT systems.
- Management of department business continuity.
- Supervision of technical IT staff.

[1] These positions may be described by varying names from department to department. It is important to include those who fill generic roles as outlined above.

- Supervision of network activity.
- Supervision of desktop services.
- Supervision of telecommunications.
- Responsibility for liaison with information technology vendors.
- The IT systems used for public communication.

1.9.2 GOVERNANCE

Executive management of the department should retain the responsibility for executive decisions that affect information technology and telecommunications. The day to day governance of information technology and telecommunications systems should be carried out by the chief of that particular operational technology.

The IT Business Continuity Plan team provides advice, information and consultation to the BCIT Manager.

1.9.3 ROLES AND RESPONSIBILITIES

i. Pre-Impact

Senior Management of IT Systems

- Ensures that the IT Business Continuity Plan is developed, maintained and updated regularly.
- Reports on the progress and status of the IT Business Continuity Plan to executive management.

Supervision of Technical IT Staff

- Continually monitors the redundancy capabilities of the computer systems and maintains a regular program of testing, training and awareness of IT business continuity principles.
- Reports regularly to the Senior Manager of IT Systems.

Supervision of Telecommunications

- Provides for monitoring of the current and ongoing condition of telecommunications systems.
- Maintains an awareness of alternate communications solutions.

Management of Department Business Continuity.

- Includes IT Business Continuity Plan principals in the development, maintenance and updating of the department Business Continuity Plan.
- Periodically checks the interface between the IT Business Continuity Plan and the department BCP to ensure compatibility between operational principles.

Responsibility for Liaison with Information Technology Vendors.

- Provides liaison between contracted IT services and the IT Business Continuity Plan team.
- Ensures vendors are aware of the impact of the department's IT Business Continuity Plan on vendor provided services.

Supervision of Network Activity

- Analyzes the capability for and availability of web redundancy.
- Ensures websites are backed up in their most current form.
- Examines and recommends web-based solutions for employee emergency notification.

Supervision of Desktop Services

- Ensures information processes are current with the requirements of the IT Business Continuity Plan.

ii. Post-impact

Senior Management of IT Systems

- Assembles the IT Business Continuity Plan team and ensures the department is aware of the circumstances surrounding the business disruption.
- Reviews recovery plan strategies with executive management.
- Authorizes all expenditures and extra personnel required to deal with the disruption.
- Manages and monitors the overall recovery process.
- Supervises a post-disruption review and lessons learned process.

Supervision of Technical IT Staff

- Assesses the damage to computer systems and the ability to provide ongoing data processing.
- Initializes and directs the response to the business disruption of the computer systems.
- Coordinates all recovery personnel and activities.
- Supervises the retrieval of all off-site system backups, manuals, equipment, documentation and data.

Supervision of Telecommunications

- Assesses damage to the telephone system and the ability to provide ongoing communications.
- Implements alternate arrangements for telephone communications.

- Provides for redundant communications in the event of non-restoration of telephone systems.
- Ensures that telephone-based emergency notification protocols are implemented.

Management of Department Business Continuity.

- Carries out response functions as designated in the department BCP.
- Ensures the maintenance of the department's essential services in relation to the IT Business Continuity Plan.

Responsibility for Liaison with Information Technology Vendors.

- Provides consultation and expertise in repair procedures.
- Assists with the acquisition of supplies and parts to effect IT system repair.
- Arranges for data recovery where required.

Supervision of Network Activity

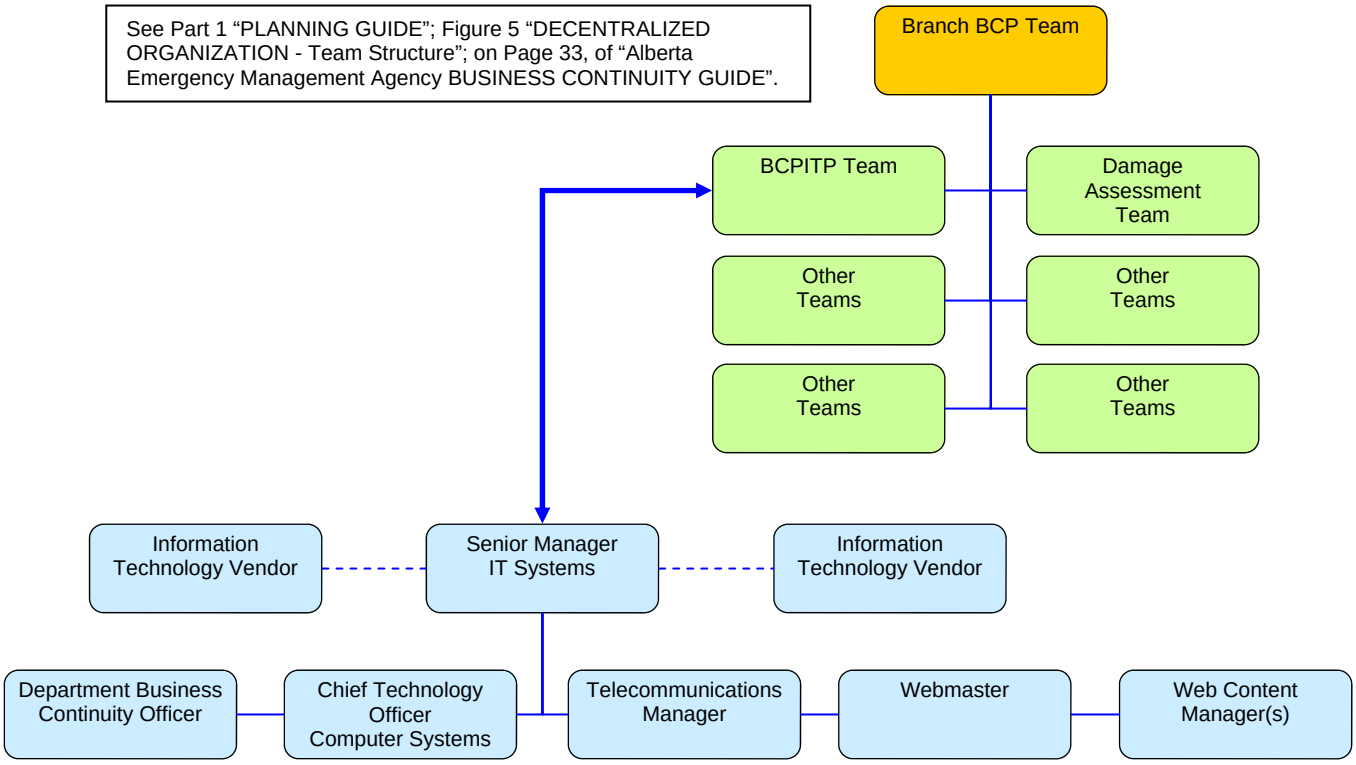
- Arranges for alternate Internet Service Providers.
- Arranges for recovery and reloading of websites.
- Ensures that web-based emergency notification systems are processed.

Supervision of Desktop Services

- Develops situation reports and updates on the current state of business disruption recovery and ensures posting to department website.

1.9.4 ORGANIZATION CHART

BUSINESS CONTINUITY INFORMATION TECHNOLOGY TEAM ORGANIZATION



1.10 KEY PLAN ASSUMPTIONS

Planning assumptions are the expectations held concerning future conditions and trends that could impact plan success. Assumptions provide a key to effective planning by reducing “time to action” (e.g.: gaining new knowledge and making it actionable so that you can plan your response to a situation before its development puts you behind the curve).

A plan for future action is based on assumptions. All assumptions, however basic, must be articulated and recorded so that the plan makes sense and can be evaluated as it is put into action. Assumptions must be clearly identified and managed, so that when the plan is activated, there is no need to go back and reevaluate or manage the original assumptions.

Departments should ensure that the assumptions made in their IT Business Continuity Plan are coordinated with assumptions of their main departmental BCP and that they reflect support provided to essential services of the department as identified in the department’s BIA.

The absence of “assumption management” is a common cause of the failure of plan strategies. All planning is based on imperfect knowledge and involves assumptions about the future that are based on available data, combined with the experience of the planning team. Most strategic plans assume certain future conditions, which is a dangerous misconception. The future is always subject to change in crazy, chaotic ways no one can anticipate. Add to this the critical nature of the business processes supported by a department’s information technology systems and uncertainty increases even more. Unless the planning team has the willingness and flexibility to redefine the assumptions when more knowledge becomes available, its plan is not likely to deliver the expected results.

Assumptions must be stated, debated and continually reevaluated as the plan goes forward. Here are a few practical steps you can take to manage your planning assumptions.

A. Understand what kind of assumptions you are making. There are four general types of planning assumptions:

   - **Cause-effect** – e.g.: *If we increase system maintenance, system reliability will increase*; or, *we do not believe more maintenance will have a measurable impact on system reliability*.
   - **Performance Expectations** – e.g.: *We expect to get a 30% percent increase in system capacity based on what we know about similar systems;* or, *We expect to have a measurable performance increase…*
   - **User Behavior Theories** – e.g.: *We believe that users care more about reliability over cost in their day-to-day operation of the system.*
   - **Trends** – e.g.: *We believe that system down time will improve as we develop better system monitoring methods.*

B. List all of your key assumptions in the appendix of your IT Business Continuity Plan. Rank the strength of each one and estimate how much of the plan is riding on each assumption. Make this list a part of your final planning document so it can be debriefed later.

C. Collect and review available data that will shed light on the validity of the assumptions. Debrief regularly to identify what went right, what went wrong and why.

D. Develop real-world exercises for the biggest risks that can prove or disprove the plan’s key assumptions.

E. Get more intelligence about what you may not be seeing in your environment before you throw more resources at the problem.

F. Plan contingencies that you can implement if course corrections are needed.

G. Increase your awareness and knowledge in areas that address important assumptions.

It is important that assumptions do not forecast events too far into the future. By definition, planning is future-oriented and the future is uncertain. We can rarely

expect to accurately foresee outcomes or precisely control developments in our environment, especially over long horizons of time.

In determining the validity of assumptions it is important to plan for unexpected changes in assumption conditions (e.g.: contingency planning). Here are some practical tips for contingency planning:

- Ensure the IT Business Continuity Plan is modular. Identify the greatest threats to the plan, or key assumptions that, if proved invalid, will nullify the plan. Develop alternative strategies that address these risks and that can be implemented without going back to the drawing board. Do not attempt to plan for every eventuality, only the most important. Planning for too many contingencies adds to the planning burden and reduces focus on the objectives.
- Identify triggers that will indicate the need to adapt or abandon the current plan. At a minimum, identify triggers that require the planning team to convene on an emergency basis to make key decisions.
- Design courses of action which permit multiple options in execution. For example, you may create specific planned alternatives or follow-on phases for likely contingencies.
- Always maintain the flexibility to pursue other options that are not planned.

It is best to think of your strategic plan as an open architecture that allows you to consider and pursue multiple possibilities. Assumptions are the foundation of a solid strategic plan and if they are flawed, the whole plan is flawed. A good plan will recognize the volatility of assumptions and will maximize freedom of action for the future by incorporating plans for contingencies.

1.10.1 SAMPLE ASSUMPTIONS

1. This plan addresses the worst-case scenario of complete disruption of (name of department)'s essential services as a result of an information technology systems interruption or destruction of a specific site(s) or facilities supporting information technology, but will also apply to less severe situations.
2. The resumption of the Department's information technology systems in the event of a disruption is linked to the department's highest priority to continue IT support to essential services as listed in the departmental BCP.
3. A designated Government of Alberta BCP cross-government coordination team will be responsible for the facilitation of cross-government coordination of certain resources and services as part of the IT protection, restoration and resumption process.
4. Current emergency response plans (e.g.:, building evacuation) are found in site-specific emergency plans and are not part of the IT process. However, given that such actions may pose a threat of

interruption to departmental IT services, these emergency plans are be included as supporting plans.

5. Regardless of circumstance, some key personnel will not be available to participate in IT continuity activities within the first 24 hours of a disruption incident.
6. The offsite (geographically separate location) storage locations housing key backed-up data are intact and accessible.
7. The department's IT vendor has a current Disaster Recovery Plan in place.
8. Existing dependencies with (list other Ministries/stakeholders) have been identified and coordinated and a current contact lists are maintained.

1.11 DEFINITIONS

It is important that all parties reading an IT Business Continuity Plan have a common understanding of the meaning of key terms, words and phrases. Departments should include a definitions section at the beginning of their plan or as a clearly identifiable annex which provides a descriptive meaning of each of these.

This list of definitions may be used as a sample list for departmental plans and provides definitions for the terms used in this guide:

Application Software	An information technology appliance which organizes and manipulates information and data in a manner which supports business communication, data storage, publication or decision making. Usual global software applications in the GoA are word processing, spreadsheet, databases, e-Mail and applications used to support telecommunications networks. Software may be commercially purchased or licensed; created by GoA personnel or persons acting on behalf of the GoA; or provided under special agreement.
Business Continuity	The procedure of planning for disruptions to business processes of a department including the identification and mitigation of risks; recovering from business disruptions; and restoring business processes to their pre-disruption state.
Business Continuity Plan (BCP)	A plan to protect business processes, recover from business disruptions and restore lost value. Each department of the GoA is required to have a BCP.

Business Disruption	A short or long term suspension of the business processes of a department as a result of an emergency or event that prevents the continuance of any or all essential services.
Business Impact Analysis	An examination of department essential services to reveal vulnerabilities, and a planning component to develop strategies for minimizing risk.
Significant Recovery Time	The length of time required to recover from a business disruption with the least amount of damage to the business processes of a department.
Data	Factual information, especially information organized for analysis or used to reason or make decisions, and computer numerical or other information represented in a form suitable for processing by computer.
Emergency	An event that requires prompt co-ordination of action or special regulation of persons or property to protect the safety, health or welfare of people or to limit damage to property.
End-user	Refers to the human executing applications on the workstation, i.e.: The ultimate user of a program, e.g.: The end user of a word processing program could be an administrative assistant or a writer. The end user of a compiler could be a software developer.
Essential Services	The services of a department defined through a Business Impact Analysis and included in the departmental Business Continuity Plan, clas.sified as either critical, vital, necessary or desired.
Facility Emergency Response Plan	A plan of the GoA to provide emergency response plans for all GOA owned and leased facilities
Information Technology (IT)	The components and systems used to transmit corporate and business information among interested parties including: • All computers with a human interface, • All computer peripherals which will not operate unless connected to a computer or network, • All voice, video and data networks and the equipment, staff and purchased services necessary to operate them, • All salary and benefits for staff whose job descriptions specifically includes technology functions, i.e.: Network services, applications development, systems administration,

	• All technology services provided by vendors or contractors, • Operating costs associated with providing information technology, and • All costs associated with developing, purchasing, licensing or maintaining software.
Internet	The network that connects computers globally.
Intranet	The network that connects computers within a specific organization or framework and limits access to specific persons.
IT Systems Failure	The failure of any information technology component for any length of time that has the potential to disrupt the business processes of a department and halt the provision of department essential services.
Local Area Network	Any information technology system used to transmit voice and data information between or among staff of a single GoA department.
Maximum Tolerable Outage	As defined in the Business Impact Analysis of a department of the GoA, it is the upper limit of time that an IT asset can be out of service before it creates an intolerable disruption to essential services or the business of a department of the GoA.
Network Server	A computer that provides a shared service to a network such as file storage, print services, network gateway, or other functions commonly shared among network users or other principals.
Operational Planning	The strategic planning process that takes place during the warning or initial impact phase of a disaster or business disruption, then is continued throughout the active operational period, to develop immediate, ongoing and long term response strategies.
Recovery Point Objective	Describes the amount of data lost measured in time. Example: If the last available good copy of data upon an outage was from 18 hours ago, then the RPO would be 18 hours.
Recovery Time Objective	The duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity.

Redundant Array of Independent (or Inexpensive) Disks	A category of disk drives that employ two or more drives in combination for fault tolerance and performance. RAID disk drives are used frequently on servers but aren't generally necessary for personal computers. RAID allows you to store the same data redundantly (in multiple paces) in a balanced ay to improve overall performance.
System Assets	The elements of an IT system as defined under “Information Technology (IT)” that support department processes and essential services.
System Reliability	The measure of the overall consistency of system support for crucial applications and essential services. Includes all aspects of system operation such as desktop support, networks, hardware, software applications and external dependencies, e.g.: electrical power.
System Restoration	Measures taken to return an IT system to its earlier basic operational state. This differs from recovery which deals with substantial retrieval of lost IT system functionality and data components.
Telecommunications	Communication at a distance by electronic transmission of voice or data by telephone or telephony networks.
Vendor (IT Vendor)	A private or publically owned organization which provides goods and services not available from within a department through a commercial purchase agreement or a mutual support arrangement.
Web (World Wide Web)	A collection of information sites located on computer hard drives connected through the internet that are used to display or supply information and provide opportunity for human interactive response.
Wide Area Network	An information technology system used to transmit voice and data information to parties or partners external to the department.

1.12 ACRONYMS

There are many acronyms that can be used in an IT Business Continuity Plan and it is essential that these be listed at the beginning of a departmental plan or within an easily identifiable annex to the plan.

This list of acronyms may be used as a sample list for departmental plans and provides definitions for the terms used in this guide.

BCP	Business Continuity Plan
BIA	Business Impact Analysis
e.g:	For example
FERP	Facility Emergency Response Plan
GoA	Government of Alberta
i.e:	that is
IT	Information Technology
MTO	Maximum Tolerable Outage
PBX	Private Branch (or Business) Exchange (Telephone System)
RAID	Redundant Array of Independent (or Inexpensive) Disks
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SDLC	System Development Life Cycle

SECTION TABLE OF CONTENTS

2. THE PLANNING GUIDE

2.1 BUSINESS IMPACT ANALYSIS

An IT System review and classification of sensitive data should be performed in conjunction with the department Business Impact Analysis to determine the adverse impact of a security occurrence in terms of loss or degradation of integrity, availability and confidentiality. This process must also identify if the types of data are subject to other regulatory requirements (e.g.: FOIP, etc).

2.1.1 PARALLELS AND RELATIONSHIP TO DEPARTMENT BIA

Based upon the departmental BIAs, the IT Business Continuity Plan should identify and rank the most crucial applications. An 'IT Applications in Support of BIA Form' is included as Appendix B in Section 3.

Table 2.2 provides examples of the potential results in the loss of applications and data.

Table 2-1: Application And Data Sensitivity Criteria

LOSS OF:	MAY RESULT IN:
Confidentiality	System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.
Integrity	System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an IT system.
Availability	If a key IT system is unavailable to its end users, the organization's mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users' performance of their functions in supporting the organization's mission.

Apply each criterion above to all systems and data and measure the impact using Table 2-2 – Magnitude of Impact. This analysis will assist in prioritizing risks and identifying areas for immediate improvement in addressing the vulnerabilities.

Table 2-2 provides examples of the magnitude of the impact of the loss.

Table 2-2: Magnitude Of Impact[1]

IMPACT	MAY RESULT IN
Low	Negotiable to minor disruption: short periodic delays to services. E.g.: The loss of some tangible assets or resources or may affect mission, reputation, or interest.
Medium	Moderate disruption; loss of service for several days. E.g.: Costly loss of tangible assets or resources, may violate, harm or impede mission, reputation, or interest, or may result in human injury.
High	Major disruption: isolation from key inputs or outputs for days or weeks. E.g.: Costly loss of major tangible assets or resources, may significantly violate, harm or impede a mission, reputation or interest, or may result in human death or serious injury.

2.1.2 ESSENTIAL SERVICES SUPPORTED AND HOW

It is important not only to list the essential services supported by IT applications, but also to demonstrate how each is supported. Using a principle of "worst case scenario" (i.e.: consider a catastrophic loss of IT system support for an essential service) develop all controls, response and recovery measures based on this standard.

A sample form is provided as Appendix C in Section 3 which can be used to develop a detailed cross reference between IT support and the Essential Services List.

2.1.3 KEY OPERATIONAL FUNCTIONS SUPPORTED

In addition to essential services, it is important to list the key operational functions of the department that are not listed as essential services but may indirectly impact on the provision of department essential services. These could include:

[1] A system or data should be considered sensitive if any of the three criteria contain a moderate or high rating.

- Purchasing
- Section Management
- Division Management
- Branch Management
- Facility Maintenance
- Purchasing
- Helpdesk
- Records Management
- Administration

This list could be quite exhaustive. Therefore, it is important to list only those functions that are key to the successful operation of a section of the department. A form of the table included in Appendix C could be used for this purpose.

2.1.4 MAXIMUM TOLERABLE OUTAGE

For purposes of this guide, “Maximum Tolerable Outage” (MTO) means the time that an IT resource (e.g.: hardware, software and telecom equipment) may be unavailable, before it prevents or inhibits the performance of a department essential service. In order to determine the MTO of IT resources, it is necessary to determine the MTO of the essential service which is supported or sustained by the IT resource. This will usually be determined by the classification of the essential service (i.e.: critical, vital, necessary, or desired) which governs the MTO according to the department Business Continuity Plan.

2.2 RISKS DEFINED / IDENTIFYING THE RISKS

Risk is the net negative impact of IT vulnerability, considering both the probability and the impact of occurrence. Risk management is the process of identifying risk, assessing risk and taking steps to reduce risk to an acceptable level. This section provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. The ultimate goal is to help GoA departments to better manage IT-related risks.

In selecting cost-effective security controls, it is important to consider that controls can be used to mitigate risk for the better protection of crucial information and the IT systems that process, store and carry this information. In managing IT-related mission risks, departments may choose to expand or abbreviate the comprehensive processes and steps suggested in this guide and tailor them to their environment.

2.2.1 OBJECTIVE

The objective of performing risk management is to enable a department to protect IT support of its essential services by:

a. Better securing the IT systems that store, process or transmit organizational information and essential services data;

b. Enabling management to make well-informed risk management decisions to justify the expenditures that are part of an IT budget; and

c. Assisting management in authorizing (or accrediting) the IT systems on the basis of the supporting documentation resulting from the performance of risk management.

2.2.2 TARGET AUDIENCE

Risk identification provides a common foundation for technical and non-technical personnel who support or use the risk management process for their IT systems. These personnel include:

- Senior management, the mission owners, who make decisions about the IT security budget;
- Chief Information Officers, who ensure the implementation of risk management for department IT systems and the security provided for these IT systems;
- IT security manager, who implements the security program;
- IT system security officers, who are responsible for IT security;
- IT system owners of system software and/or hardware used to support IT functions;
- Information owners of data stored, processed and transmitted by the IT systems;
- Business or functional managers, who are responsible for the IT procurement process;
- Technical support personnel (e.g.: network, system, application and database administrators; computer specialists; data security analysts), who manage and administer security for the IT systems;
- IT system and application programmers, who develop and maintain code that could affect system and data integrity;
- IT quality assurance personnel, who test and ensure the integrity of the IT systems and data;
- Information system auditors, who audit IT systems; and
- IT consultants, vendors and service providers, who support the department in risk management.

2.2.3 IMPORTANCE OF RISK MANAGEMENT

Risk management encompasses three processes: risk assessment, risk mitigation, and evaluation and assessment. The system manager is responsible for determining whether the remaining risk is at an acceptable level or whether additional security controls should be implemented to further reduce or eliminate the remaining risk before authorizing (or accrediting) the IT system for operation.

Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their department's mission. This process is not unique to the IT environment; it pervades decision-making in all areas of department operation. Take the case of building security, for example. Many building operators decide to have building security systems installed and pay a monthly fee to a service provider to have these systems monitored for the better protection of the property. Presumably, the building operators have weighed the cost of system installation and monitoring against the value of department assets and employee safety, a fundamental "mission" need.

The head of an organizational unit must ensure that the department has the capabilities needed to accomplish its mission. These mission owners must determine the security capabilities that their IT systems must have to provide the desired level of mission support in the face of real world threats. If the department has a tight budget for IT security, IT security spending must be reviewed as thoroughly as other management decisions. A well-structured risk management methodology, when used effectively, can help management identify appropriate controls for providing the mission-essential security capabilities.

2.2.4 INTEGRATION OF RISK MANAGEMENT INTO SDLC

Minimizing negative impact on an organization and the need for sound decision-making practices are the fundamental reasons departments should implement a risk management process for their IT systems. Effective risk management must be totally integrated into the System Development Life Cycle (SDLC). An IT system's SDLC has five phases: initiation, development or acquisition, implementation, operation or maintenance and disposal. In some cases, an IT system may occupy several of these phases at the same time. However, the risk management methodology is the same regardless of the SDLC phase for which the assessment is being conducted. Risk management is an iterative process that can be performed during each major phase of the SDLC.

SDLC phases consist of:

- Phase 1 – Initiation
- Phase 2 – Development or Acquisition

- Phase 3 – Implementation
- Phase 4 – Operation or Maintenance
- Phase 5 – Disposal

Table 2-3 contains a description of the characteristics of each SDLC phase and indicates how risk management can be performed in support of each phase.

Table 2-3: Integration of Risk Management into the SDLC

SDLC PHASES	PHASE CHARACTERISTICS	SUPPORT FROM RISK MANAGEMENT ACTIVITIES
Phase 1 – Initiation	The need for an IT system is expressed and the purpose and scope of the IT system is documented.	• Identified risks are used to support the development of the system requirements, including security requirements and a security concept of operations (strategy).
Phase 2 – Development or Acquisition	The IT system is designed, purchased, programmed, developed or otherwise constructed.	• The risks identified during this phase can be used to support the security analyses of the IT system that may lead to architecture and design trade-offs during system development.
Phase 3 – Implementation	The system security features should be configured, enabled, tested and verified.	• The risk management process supports the assessment of the system implementation against its requirements and within its modeled operational environment. Decisions regarding risks identified must be made prior to system operation.
Phase 4 – Operation or Maintenance	The system performs its functions. Typically the system is being modified on an ongoing basis through the addition of hardware and software and by changes to organizational processes, policies and procedures.	• Risk management activities are performed for periodic system reauthorization (or reaccreditation) or whenever major changes are made to an IT system in its operational, production environment (e.g.: new system interfaces).

Phase 5 – Disposal	This phase may involve the disposition of information, hardware and software. Activities may include moving, archiving, discarding or destroying information and sanitizing the hardware and software.	• Risk management activities are performed for system components that will be disposed of or replaced to ensure that the hardware and software are properly disposed of, that residual data is appropriately handled and that system migration is conducted in a secure and systematic manner.

2.2.5 KEY ROLES

Risk management is a management responsibility. This section describes the key roles of the personnel who should support and participate in the risk management process.

- **Senior Management** – Senior management, under the standard of due care and ultimate responsibility for mission accomplishment, must ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the mission. They must also assess and incorporate results of the risk assessment activity into the decision making process. An effective risk management program that assesses and mitigates IT-related mission risks requires the support and involvement of senior management.
- **Chief Information Officer (CIO)** – The CIO is responsible for the department's IT planning, budgeting and performance including its information security components. Decisions made in these areas should be based on an effective risk management program.
- **System and Information Owners** – The system and information owners are responsible for ensuring that proper controls are in place to address integrity, confidentiality and availability of the IT systems and data they own. Typically, the system and information owners are responsible for changes to their IT systems. Thus, they usually have to approve and sign off on changes to their IT systems (e.g.: system enhancement, major changes to the software and hardware). The system and information owners must therefore understand their role in the risk management process and fully support this process.
- **Business and Functional Managers** – The managers responsible for business operations and the IT procurement process must take an active role in the risk management process. These managers are the individuals with the authority and responsibility for making the trade-off decisions essential to mission accomplishment. Their involvement in the risk management process enables the achievement of proper security for the IT systems, which, if managed properly, will provide mission effectiveness with a minimal expenditure of resources.

- **Information System Security Officers** – IT security program managers and computer security officers are responsible for their department's security programs, including risk management. Therefore, they play a leading role in introducing an appropriate, structured methodology to help identify, evaluate and minimize risks to the IT systems that support their organizations' missions. They also act as major consultants in support of senior management to ensure that this activity takes place on an ongoing basis.
- **IT Security Practitioners and Vendors** – IT security practitioners (e.g.: network, system, application and database administrators; computer specialists; security analysts; security consultants) are responsible for proper implementation of security requirements in their IT systems. As changes occur in the existing IT system environment (e.g.: expansion in network connectivity, changes to the existing infrastructure and organizational policies, introduction of new technologies), the IT security practitioners must support or use the risk management process to identify and assess new potential risks and implement new security controls as needed to safeguard their IT systems.
- **Security Awareness Trainers** (Security/Subject Matter Professionals) – The organization's personnel are the users of the IT systems. Use of the IT systems and data according to an organization's policies, guidelines and rules of behaviour is key to mitigating risk and protecting the organization's IT resources. To minimize risk to the IT systems, it is essential that system and application users be provided with security awareness training. Therefore, the IT security trainers or security/subject matter professionals must understand the risk management process so that they can develop appropriate training materials and incorporate risk assessment into training programs to educate the end users.

2.2.6 RISK ASSESSMENT

Risk assessment is the first process in the risk management methodology. Organizations use risk assessment to determine the extent of the potential threat and the risk associated with an IT system throughout its SDLC. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process.

Risk is a function of the *likelihood* of a given *threat-source's* exercising a particular potential *vulnerability*, and the resulting *impact* of that adverse event on the department.

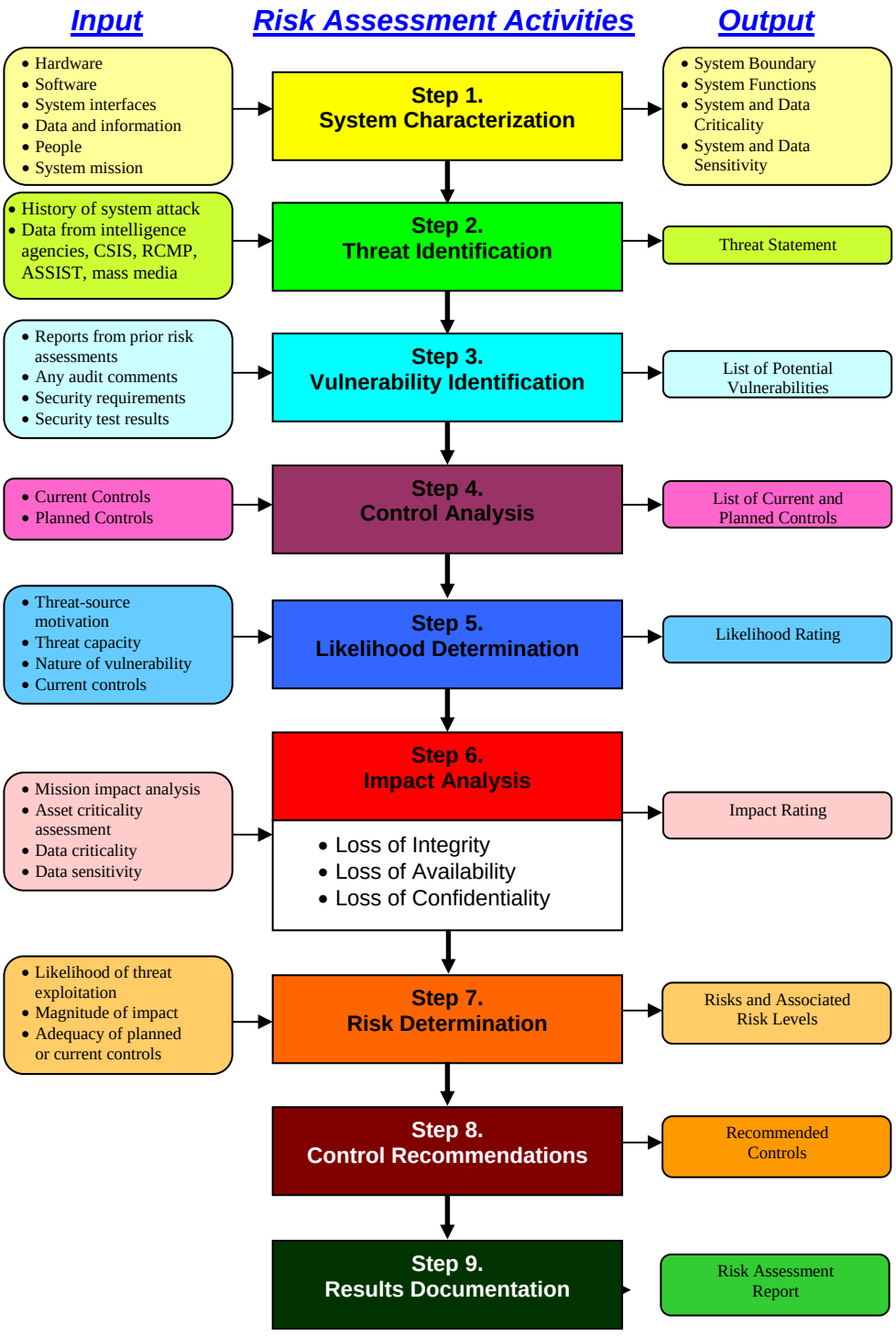
To determine the likelihood of a future adverse event, threats to an IT system must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the IT system. Impact refers to the magnitude of harm that could be caused by a threat's exercise of vulnerability. The level of impact is governed by the potential mission impacts and in turn produces a relative value for the IT

assets and resources affected (e.g.:, the criticality and sensitivity of the IT system components and data). The risk assessment methodology encompasses nine primary steps:

- Step 1 – System Characterization
- Step 2 – Threat Identification
- Step 3 – Vulnerability Identification
- Step 4 – Control Analysis
- Step 5 – Likelihood Determination
- Step 6 – Impact Analysis
- Step 7 – Risk Determination
- Step 8 – Control Recommendations
- Step 9 – Results Documentation

Steps 2, 3, 4, and 6 can be conducted in parallel after Step 1 has been completed. Figure 2-1 contains a Risk Assessment Methodology Flowchart which depicts these steps and the inputs to and outputs from each step.

Figure 2-1: Risk Assessment Methodology Flowchart



[1] A "Risk Assessment Report" outline is included in Appendix A.

A Risk Assessment Report should include the following components:

- Introduction
- Risk Assessment Approach
- System Characterization
- Threat Statement
- Risk Assessment Results
- Summary

A Risk Assessment Report Form is included as Appendix A in Section 3.

2.3 APPLICATION SYSTEM IMPACT STATEMENTS

Interviews should be held with heads of operating sections of the department resulting in a narrative of the effect of a system outage or loss of application software assuming a worst-case scenario for each operational section. Summaries of the narratives would be included in the IT Business Continuity Plan and the full result of the interview should be filed. The narrative indicates the operational section's dependency on computer support and indicates the critical time frame that the section can be without the system or an application's functionality.

2.3.1 CONNECTED TO THE BIA

Application System Impact Statements should be connected to the output of the department BIA and are used to classify each application into the categories of critical, vital, necessary or desired.

- **Critical** (Highest Priority)

  Information technology supporting GoA essential services is considered "critical" if its loss would affect the department's ability to maintain an essential service classified as critical. The system or application must be restored within 24 hours.

- **Vital** (Second Highest Priority)

  Information technology supporting GoA essential services is considered "vital" if its loss would affect the department's ability to maintain an essential service classified as vital. The system or application must be restored within 72 hours.

- **Necessary** (Third Highest Priority)

  Information technology supporting GoA essential services must be restored within two weeks for those essential services classified as "necessary". Delay

beyond the time frame could result in extended loss incurring disproportionate recovery costs.

- **Desired** (Lowest Priority)

  Restoration of information technology supporting GoA essential services classed as “desired” can be set aside for two weeks or longer, but must be returned to normal operation condition as soon as possible in order to avoid further disruption of desired services.

In instances where specific information technology pieces support more than one classification of essential services they should be restored using the priority of the highest classification level.

2.3.2 OPERATIONAL BRANCH AND UNIT DEPENDENCIES

In maintaining the support of essential services the issue of dependency between an information technology application and a branch or unit of the department maintaining an essential service is crucial. In every case of multi-service disruption there will be the need to set priorities for the assignment of resources and, while one branch or unit may be more dependent upon information technology than another, it is important to make the decision to assign resources based solely upon the essential services affected.

In order to assign IT resources to a task, the following steps must be performed.

a. **Identify task requirement** – What is the task and which essential service does the task impact?

b. **Identify necessary resources** – The resources needed by a task must be identified. For example, determining in which module of the system a bug appears identifies the resources needed by that task e.g.: an engineer with expertise in that module).

c. **Identifying available resources** – What resources are available in light of other, possibly greater, department priorities?

d. **Choosing a resource** – One particular resource must be chosen. To choose a particular resource from those available requires some way to evaluate how good a particular resource will be for the task. Obviously, there are many possible bases for making this decision, such as speed, quality, availability, motivation, etc. For example, assigning bug reports to the next free engineer is a way to choose a particular resource based on availability rather than expertise. Which criteria to use, will depend on the nature of tasks being coordinated.

e. **Identify when resources will be available** – In some cases, it is important to consider when the resources are available, especially if multiple resources are required at the same time. In this case, the choice depends on when the required resources are free.

f. **Assigning resources** – Finally, the assignment of the resource must be communicated to the individual performing the task. As well, for non-shareable resources, the resource must be marked as "in use" or other assigners warned to avoid conflicting assignments.

2.3.3 IT BUSINESS IMPACT ANALYSIS

Example 2.1 provides a summary of the Application System Impact Statements, outlining the period of time before an application's loss becomes critical and classifying each application as critical, vital, necessary or desired. An IT Business Impact Analysis Matrix is included as Appendix D in Section 3.

Example 2.1: IT Business Impact Analysis Matrix

Application	0 - 24 hrs[5]	0 - 72 hrs[1]	0 - 14 days[1]	0 - 14+ days[1]	Recovery Priority[6]	ES Classification
Email	MN	MN	MN	MO	4	Desired
Employee Info Database	MN	MN	MN	MN	5	Desired
Fileserver	CR				1	Critical
General Business Applications	MN	MO	MO	CR	3	Necessary
Monthly Support Cheques	MO	CR			2	Vital

By using the above table, we see that the priority in a phased recovery strategy is as follows:

Fileserver	24 hours or less
Monthly Support Cheques	72 hours or less
General Business Apps	2 weeks or less
Email	2 weeks or more, however before Employee Info Database
Employee Info Database	2 weeks or more

[5] Critical time frames are measured from zero to ensure a standardized priority rating. These columns should reflect he severity of the failure of IT applications on essential service using the scale – **MN** = Minimum Impact; **MO** = Moderate Impact; and **CR** = Critical Impact.
[6] Assign a recovery priority based on the number "1" as highest. This allows for priorization of essential services in the same classification.

2.4 PROTECTION STRATEGIES

Today almost every major business process of the GoA relies on information technology. It is important to ensure that data protection and recovery strategies have adapted to this intensive dependence on computer-based systems and data processing. The policies and practices need to meet your department's current business continuity and disaster recovery requirements and satisfy auditors' demands about information security and retention.

Departments have a range of options for data backup to address their diverse business challenges. Online backup, for example, can be a significant part of a department's entire backup, retention and security strategy, or it may supplement existing backup technologies and processes, such as tape.

In fact, there may be no single right choice for system protection. Many large organizations, for instance, have special availability requirements for their most crucial applications, but different requirements for other types of data.

For mission-crucial applications, for example, tape is an excellent, exceptionally cost-effective method for getting a truly diverse, statistically important additional tier of data protection. Unlike replication-based solutions, tape provides diversity across many dimensions – physical isolation, media diversity, off-line storage and format independence – and dramatically reduces the chance that a problem with the primary data will impact the backup data.

2.4.1 PRE-LOSS MEASURES TAKEN TO PROTECT CRUCIAL SYSTEMS

In every business continuity consideration of information technology, there is far more benefit realized by protection of essential IT systems from failure than recovery from a systems breakdown. This protection needs to be applied in several areas of IT operation.

- **System planning** – Making certain that an overall development plan exists for the current needs and future growth of your department's information technology systems.
- **Current technology** – Ensuring that changes and patches to your IT systems are compatible with its existing technology.
- **Preventive maintenance** – Developing and maintaining a sound preventive maintenance program that allows for anticipation of equipment failures and deviations from unassailable operation.
- **System redundancy** – Ensuring that cost effective options are available for alternate operation of system applications and hardware.
- **Data backup** – A regular program of offsite data storage of sufficient frequency to ensure that lost data can be retrieved in a timely fashion.

1. Measures Application Review Cycles & Time Frame

In successful protection of IT systems, the only effective measure taken is the last one. It is important to ensure that pre-loss measures are applied on a time regularized basis. Examples of time frames for pre-loss measures are demonstrated in Example 2.2. A 'Time Frames for Pre-Loss Measures' Form as Appendix E is included in Section 3.

Example 2.2: Time Frames For Pre-Loss Measures

MEASURE	DAILY	WEEKLY	MONTHLY	YEARLY	OTHER
System planning					
Planning Measure 1		x			As required
Planning Measure 2			x		
Current technology					
Patch 1		x			As required
Patch 2				x	
Preventive maintenance					
Maintenance Task 1	x				
Maintenance Task 2		x			
System redundancy					
Redundancy check 1		x			
Redundancy check 2			x		
Data backup					
Application configuration		x			
Live data	x	x			
Repository data			x		

Prior to selecting a protection strategy, a department should refer to its organization business continuity plan which should indicate the key metrics of Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for various business processes such as the process to run payroll, generate an order, etc. The metrics specified for the business processes must then be mapped to the underlying IT systems and infrastructure that support those processes.

Once the RTO and RPO metrics have been mapped to IT infrastructure, the department can determine the most suitable recovery strategy for each system. An important note here however is that the business ultimately sets the IT budget and therefore the RTO and RPO metrics need to fit with the available budget. While most business unit heads would like zero data loss and zero time loss, the cost associated with that level of protection may make the desired high availability solutions unpractical.

The following is a list of the most common strategies for data protection.

- Backups made to tape and sent off-site at regular intervals (preferably daily);
- Backups made to disk on-site and automatically copied to off-site disk, or made directly to off-site disk;
- Replication of data to an off-site location, which overcomes the need to restore the data (only the systems then need to be restored or synced), generally making use of Storage Area Network (SAN) technology; and
- High availability systems which keep both the data and system replicated off-site, enabling continuous access to systems and data.

In many cases, a department may elect to use an outsourced Disaster Recovery Provider to provide a stand-by site and systems rather than using their own remote facilities.

In addition to preparing for the need to protect or recover systems, departments must also implement precautionary measures with an objective of preventing a disaster situation in the first place. These may include some of the following:

- Local mirrors of systems and/or data and use of disk protection technology;
- Surge Protectors to minimize the effect of power surges on delicate electronic equipment;
- Uninterruptible Power Supply (UPS) and/or Backup Generator to keep systems going in the event of a power failure;
- Fire Preventions (e.g.: more alarms, accessible fire extinguishers); and
- Anti-virus software and other security measures.

2.4.2 MEASURES VERIFICATION PROCESS

You can never let your guard down. You can divide up your data, wipe your data and encrypt your data, but that does not necessarily mean your data is safe from intrusion. Constant vigilance of your systems, your procedures and your people working on those systems is the price of computer security today. If you are not willing to pay that price, you may just find yourself in the daily headlines.

The accreditation of an IT System is the official management decision to permit operation of a specified environment at an acceptable level of risk, based on the implementation of an approved system configuration management program. The configuration management program should be verified on a regular basis.

The IT System should be reaccredited whenever changes are made. Proposed modifications to an IT System should be reviewed by the senior official responsible for IT systems to determine if the proposed modifications will impact the protections on the system. If the protection aspects of the system's environment change, if the applicable IT protection requirements change, or if the protection mechanisms implemented for the system change, the system needs be reaccredited.

All modifications to IT relevant resources (including software, firmware, hardware, or interfaces and interconnections to networks) should be reviewed and approved in accordance with procedures prior to implementation. All IT relevant changes should be subject to the provisions of the system configuration management program.

Regular tests should be carried out on the department's IT Systems to verify the pre-loss measures are documented and demonstrated for audibility.

2.5 RECOVERY STRATEGIES

Restoration and recovery strategies developed should be based on the results of the BIA, including the critical time frames and available alternative manual procedures in the event of an extended computer coverage. Strategies should be based on a "worst case" scenario, since planning for such events always allows margins for dealing with lesser incidents of business disruption. Strategies should also be developed to respond to "all hazards", e.g.: failure of systems due to software corruption, hardware component failure, or external forces such as an extended power failure.

2.5.1 APPROACHES

The recovery time frame is the basis for selecting a recovery strategy in a worst case scenario. Example 2.3 provides a sample of strategy selection based on a critical time frame using three sample strategies[7]:

1. Recovery` of media with backed up system applications and data,
2. Activation of an alternate network operations site, and

[7] Selection of a recovery strategy would always be based upon the actual IT processing need of the essential service. E.g.: if a critical service did not require a network connection, then strategy 2 (activation of an alternate network operations site) would not need to be employed to recover that service.

3. Switching to manual business recording procedures.

A 'Strategy Selection Based on Recovery Time Frames of Essential Services' Form is included as Appendix F in Section 3.

Example 2.3: Strategy Selection Based on Recovery Time Frames of Essential Services

	Expected Outage Time			
Essential Service	**<24hrs**	**>24hrs - <72hrs**	**>72hrs - <2wks**	**>2wks**
Critical Service 1	Strategy 1	Strategy 2	Strategy 3	Strategies 1, 2, 3
Critical Service 2	Strategy 1	Strategy 1	Strategy 1	Strategy 1
Vital Service 1		Strategy 3	Strategy 1	
Vital Service 2		Strategy 1	Strategy 2	Strategies 1,2
Vital Service 3			Strategy 3	
Necessary Service 1			Strategy 1	Strategy 3
Necessary Service 2			Strategy 2	
Desired Service 1				Strategy 1
Desired Service 2			Strategy 1	
Desired Service 3				Strategy 3

2.5.2 ESCALATION FRAMEWORK

The factors and variables surrounding a disaster or business disruption from any cause should not be expected to remain static. As an incident progresses, it will create conditions that require either an escalation or a de-escalation of strategies in either selection or intensity.

Examples of the factors that change an incident requiring an escalation or de-escalation of strategies are:

- Time of availability of repair or replacement parts.
- An interface between critical services causing an increase or decrease in the criticality of one or the other, e.g.: a loss of desktop services escalates into a loss of network.
- Public or political pressure on a department to restart a critical service whose absence causes human angst, e.g.: cheques unavailable to a special needs group.
- Potential further damage to additional IT systems, e.g.: removal of viruses or malware before further contamination.

- Potential further loss of data without system recovery, e.g.: data continues to be gathered manually increasing the risk of loss of a hastily arranged paper trail.

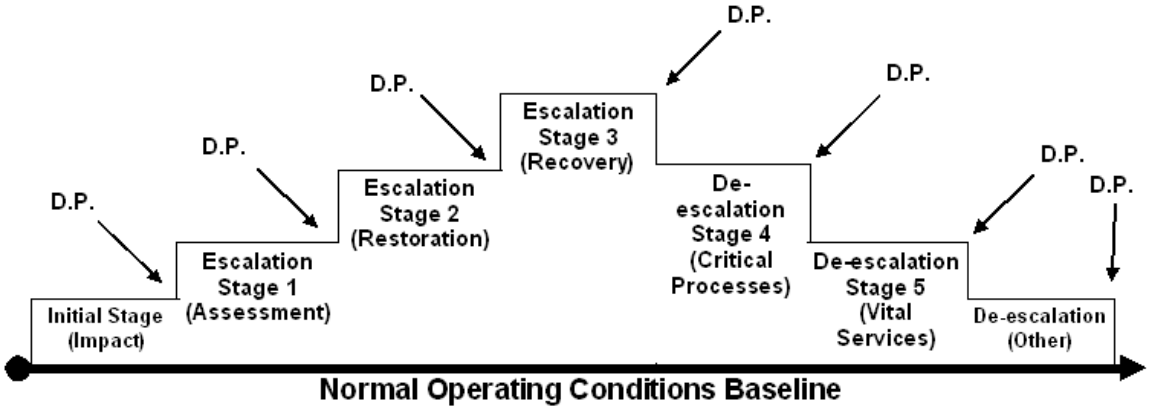
The escalation of strategies will depend upon variables that need to be recognized by the development of decision points.

2.5.3 DECISION POINTS

A decision point is the beginning position of a stage in a recovery framework in which opportunity exists for choosing and rationalizing strategies chosen to deal with that stage of recovery. It is helpful during the operational planning phase to identify the immediate and potential decision points at which measures can be escalated or de-escalated as required.

Decision points are like stair steps in a recovery framework as demonstrated in Figure 2-3 “Decision Points Illustrated”.

Figure 2-3 Decision Points Illustrated



Decision points are the staging points at which each phase of the operational planning cycle is reviewed, reassessed, realigned and revised.

2.5.4 DATA SALVAGE METHODOLOGIES

The success of data recovery and salvage will depend to a great degree upon the “protection methods” applied to a department’s IT system as outlined in section 2.4. However, should a system failure occur as a result of any of the following hazards, the restoration of the system and recovery of data will become key issues.

i. Data System Maintenance Hazards

Examples of data system maintenance hazards include:

- Unexpected failure of data storage media, e.g.: Hard Drive, removable storage media
- Damage to data storage media, e.g.: water, fire, heat, smoke
- Software Failure & corruption
- Power Outage, Electrical shortage
- Human Error
- Virus Damage & Repair
- Vandalism & Sabotage

There are three types of damage that can affect an IT system and stored data.

1. **Physical Damage** – Recovering data from physically damaged hardware can involve multiple techniques. Some damage can be repaired by replacing parts in the hard disk. This alone may make the disk usable, but there may still be logical damage. A specialized disk imaging procedure may need to be used to recover every readable bit from the surface. Once this image is acquired, the image can be analyzed for logical damage and will possibly allow for much of the original file system to be reconstructed.
2. **Logical Damage** – Far more common than physical damage is logical damage to a file system. Logical damage is primarily caused by power outages that prevent file system structures from being completely written to the storage medium, but problems with hardware (especially RAID controllers) and drivers, as well as system crashes, can have the same effect. The result is that the file system is left in an inconsistent state. This can cause a variety of problems, such as strange behaviour (e.g.:, infinitely recursing directories, drives reporting negative amounts of free space), system crashes, or an actual loss of data. Various programs exist to correct these inconsistencies, and most operating systems come with at least a rudimentary repair tool for their native file systems.
3. **Overwritten Data** – Many operating systems, file managers, and other software provide a facility where file are not immediately deleted when the user requests that action. Instead, the file is moved to a holding area, to allow the user to easily revert a mistake. Even when an explicit deleted file retention facility is not provided or when the user does not use it, most computers do not actually remove the contents of a file when it is deleted[8].

[8] Data remanence is the residual representation of data that has been in some way been nominally erased or removed. This residue may be due to data being left intact by a nominal delete operation, or through physical properties of the storage medium. Data remanence may make inadvertent disclosure of sensitive information possible, should the storage media be released into an uncontrolled environment (e.g.:, thrown in the trash, or given to a third-party). Various techniques have been developed to counter data remanence. Depending on the effectiveness and intent, they

Instead, they simply remove the file's entry from the file system directory. The contents of the file -- the actual data -- remain on the storage medium. The data will remain there until the operating system reuses the space for new data. In some systems, enough file system metadata is also left behind to enable easy undeletion by commonly available utility software. Even when undelete is not possible, until the actual data is overwritten, it can be read by software that reads disk sectors directly. Computer forensics often employs such software.

2.6 RECOVERY STRATEGIES

Due to the heavy reliance of a department on technology and the extensive impact on users, the urgency of the restoration of IT systems increases exponentially during system outages. This urgency can be dealt with by response escalation.

Escalation methods consist of two actions:

1. Hierarchical escalation - passing information and requesting decision or action on an incident, problem or change to more senior staff; and
2. Functional escalation - applying other resources and expertise to the recovery.

The circumstances in which either vertical escalation for information/authority to apply further resources or horizontal escalation for greater functional involvement need to be precisely described, so that the purpose of the escalation and the nature of the required response is absolutely clear to all parties as the escalation occurs. Escalation rules will be geared to the recovery time objectives of priority essential services as designated in the department Business Continuity Plan.

Hierarchical escalation should always commence at the time of initial outage to create an awareness of the need for decision making and possible resources that might be required in the restoration process.

2.6.1 ALTERNATE LOCATIONS AND TIMELINES

Altering the location of the recovery operation or recovery time objective are two of the more common functional escalation methods.

- Alternate locations for recovery and operation of important system components (e.g.: alternate network server) can be used when it becomes apparent that the first or normal location for operation is not suitable for a successful recovery within the timelines outlined in the department BIA for

---

are often classified as either clearing or purging/sanitizing. Specific methods include overwriting, degaussing, encryption, and physical destruction.

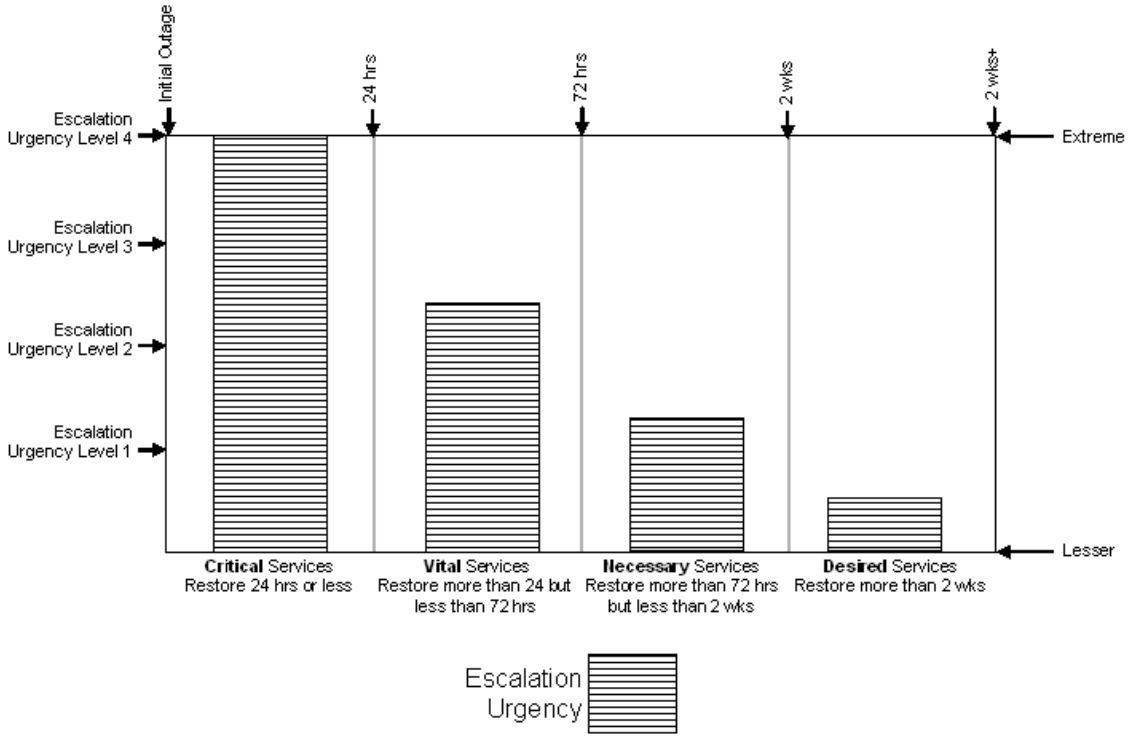
restoring essential services supported by the IT system. Some factors that can prompt a move to an alternate location are:

- Extended loss of utility services, e.g.: power, communications.
- Extensive damage to the physical facility.
- Loss of access to the location.
- Any other factor that creates a loss of system support at a specific location.

- The recovery time objective may be altered due to one of two factors:
  - An extended loss of the system creates the potential for an extended loss of a critical essential service and the timeline for recovery would be moved up; or
  - The priority of one essential service over another means the recovery time of the system supporting the service with the lesser priority would have to be pushed back.

Figure 2-4 illustrates the urgency of escalating recovery operations depending upon the criticality of the services affected versus the projected length of system outage.

Figure 2-4 Timeline Escalation for System Recovery



2.6.2 METHOD CHANGES AND TIMELINES

Escalation can also mean changing the methods and techniques used to recover an IT system failure. There are two paths to recovery from an IT system failure, data recovery and system restoration.

- **Data Recovery** – Damage to data can take two forms, physical and logical.
  - A wide variety of failures can cause physical damage to storage media. CD-ROMs can have their metallic substrate or dye layer scratched off; hard disks can suffer any of several mechanical failures, such as head crashes and failed motors; tapes can simply break. Physical damage always causes at least some data loss, and in many cases the logical structures of the file system are damaged as well. This causes logical damage that must be dealt with before any files can be salvaged from the failed media. Most physical damage cannot be repaired by end users.
  - Far more common than physical damage is logical damage to a file system. Logical damage can be caused by power outages, computer virus infections, hacker intrusions, etc., that prevent file system structures from being correctly written to the storage medium, but problems with hardware and drivers, as well as system crashes, can have the same effect. The result is that the file system is left in an inconsistent state.
- **System Restoration** – The effectiveness of system restoration methods depends upon the system point of failure. There are eight monitoring points that will help ensure system health and restoration.
  - Monitoring hard disks for errors
  - Monitoring used/free disk space
  - Monitoring build-up of unnecessary files
  - Monitoring hard disk fragmentation
  - Establishing and monitoring system restore points
  - Monitoring file backup systems
  - Monitoring application of updates and security patches
  - Periodically reviewing event viewer logs

Response escalation can be achieved on either path by the application of alternate locations and timelines, or method changes and timelines.

2.6.3 WORST-CASE SCENARIOS

Over response through the application of worst-case scenario solutions can often provide a legitimate means to escalate response to a system failure. The following scenarios provide examples.

- In a worst-case scenario, server hardware fails and cannot be recovered. To return to operations, you must have a complete backup of the server that you can restore to a new piece of hardware. This complete backup will include data stored on the server, applications, and the operating system itself. Several of your department's critical services are affected and may not be able to be restored in their RTO framework.

  An escalation *of server restoration time would be effective in this case.*

- You've worked hard to configure and maintain a best practice server environment. You have outfitted the server with a sophisticated RAID subsystem, carefully managed file and share permissions, locked down the server with policy, and physically secured the server to prevent unauthorized interactive log on. But today, none of that matters, because the building's fire sprinklers went off last night, and today your servers are full of water. All that matters today is that you are able to restore your data from backup.

  In this case serious consideration should be given to relocating server applications.

- Freezing rain knocks out power over a wide area. The power transmission infrastructure suffers major damage and a realistic estimate of power restoration is impossible to predict. The backup generator in your facility is activated; however, it becomes clear that it will soon run out of fuel. Due to the widespread power outage fuel supplies are scarce as a number of facilities have activated their generators.

  A change in escalation methodology might be effective here - changing to a manual system until the power comes back on.

2.7 KEY SYSTEMS

A computer system, which may be made up of multiple individual systems and components, designed to provide support to Government of Alberta essential services must be able to perform in a consistent and timely manner under various operating conditions. It must be able to meet its goals and objectives whether it is in a state of normal operation or under some sort of stress or in a hostile environment. Components of survivable computer systems can be very complex and far reaching.

Survivability of computer systems and computer security are in many ways related but at a low-level very much different. For instance, the hardening of a particular system to be resistant against intelligent attacks may be a component of a

survivable computer system. It does not address the ability of a computer system to fulfill its purpose when it is impacted by an event such as a deliberate attack, natural disaster or accident, or general failure. A survivable computer system must be able to adapt, perform its primary key functions even if in a hostile environment, even if various components of the computer system are incapacitated, or in some cases, even if the entire "primary" system has been destroyed.

As an example; a system designed to provide real-time key information regarding analysis of specialized medications ceases to function for a few hours because of wide spread loss of communication. However, it maintains the validity of the data when communication is restored and systems come back online. This computer system could be considered to have survived under conditions outside of its control. On the other hand, the same system fails to provide continuous access to information under normal circumstances or operating environment, because of a localized failure, may not be judged to have fulfilled its purpose or met its objective.

Many computer systems are designed with fault tolerant components so they continue to operate when key portions of the system fail. For instance; multiple power supplies, redundant disk drives or arrays, even multiple processors and system boards that can continue to function even if its peer component is destroyed or fails. The probability of all components designed to be redundant failing at one time may be quite low. However, a malicious entity that knows how the redundant components are configured may be able to engineer failures across the board rendering the fault tolerant components ineffective.

High availability also plays a role in a survivable computer system. However this design component may not maintain computer system survivability during certain events such as various forms of malicious attack. An example of this might be a key web service that has been duplicated, say across multiple machines, to allow continuous functionality if one or more the individual web servers was to fail. The problem is that many implementations of high availability use the same components and methodology on all of the individual systems. If an intelligent attack or malicious event takes place and is directed at a specific set of vulnerabilities on one of the individual systems, it is reasonable to assume the remaining computer systems that participate in the highly available implementation are also susceptible to the same or similar vulnerabilities. A certain degree of variance must be achieved in how all systems participate in the highly available implementation.

Contemporary large-scale networked systems that are highly distributed improve the efficiency and effectiveness of organizations by permitting new levels of organizational integration. However, such integration is accompanied by elevated risks of intrusion and compromise. These risks can be mitigated by incorporating survivability capabilities into an organization's systems. As an emerging discipline, survivability builds on related fields of study (e.g.:, security, fault tolerance, safety, reliability, reuse, performance, verification, and testing) and introduces new

concepts and principles. Survivability focuses on preserving essential services in unbounded environments, even when systems in such environments are penetrated and compromised.

2.7.1 KEY SYSTEMS AND HARDWARE/SOFTWARE COMPONENTS

One of the most important issues for survivability is knowing what are the key systems that support GoA essential services and the hardware and software components that make up each of them. Example 2.4 illustrates a method for tracking the reliability of GoA essential services on the key systems that support them. A 'Table of Key Systems and hardware/Software Components' Form is included as Appendix G in Section 3.

Example 2.4: Table of Key Systems and Hardware/Software Components[9]

Essential Service	Category	System Name / Identity	Hardware Components[10]	Software Applications[2]	Survivability Components[2]
Client Financial Support	*Critical*	*Financial Controls Interface*	• *15Gb IBM server* • *Cisco Integrated Router*	• *VALID Finance Tracking* • *Standard MS Office Excel*	• *230V 3 phase UPS* • *Redundant Cisco Integrated Router*
Hazardous Waste Pesticide Mgmt.	*Vital*	*HazWas Data Tracking*	• *3Gb RAID Partition* • *D-Link ADSL Modem*	• *ALPHA 5 Ver. 8 web data storage* • *Standard MS Office Project Mgmt.*	• *Replicant data storage ALPHA* • *Alternate web server contract*

2.7.2 NETWORK KEY SYSTEMS

Society is growing increasingly dependent upon large-scale, highly distributed systems that operate in unbounded network environments. Unbounded networks, such as the Internet, have no central administrative control and no unified security policy. Furthermore, the number and nature of the nodes connected to such networks cannot be fully known. Despite the best efforts of security practitioners, no amount of hardening can assure that a system that is connected to an unbounded network will be invulnerable to attack. The discipline of survivability can help ensure that such systems can deliver essential services and maintain

[9] Data in table cells is typical data for example only.
[10] Provide as much detail as possible about individual components.

essential properties such as integrity, confidentiality, and performance, despite the presence of intrusions. Unlike traditional security measures, which require central control and administration, survivability is intended to address unbounded network environments. This section describes the survivability approach to helping assure that a system that must operate in an unbounded network is robust in the presence of attack and will survive attacks that result in successful intrusions. Considerations of survivability as an integrated engineering framework, the current state of survivability practice, the specification of survivability requirements, and strategies for achieving survivability are important in measuring network criticality.

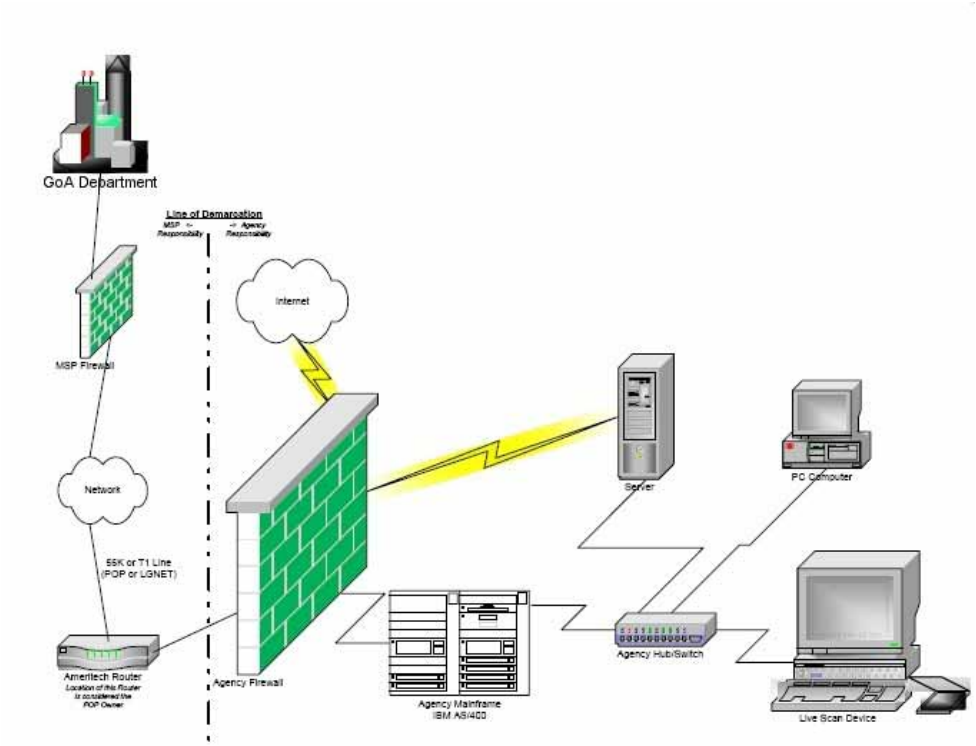
Security without compromising usability is the challenge facing network administrators. There are two considerations:

- The system must be useable by a variety of people with different job requirements and a wide range of computer understanding. There is no point in locking down a system against security breaches if it compromises its utility to its end users.
- Protection from a wide variety of accidents, attacks and intrusions to keep the data safe. Sensitive data can be easily compromised in today's computer systems and networks especially in view of network interconnections on a global scale.

Network security problems can be divided roughly into four intertwined areas: confidentiality, authentication, nonrepudiation, and integrity control.

- Confidentiality has to do with keeping information out of hands of unauthorized users.
- Authentication deals with determining whom are talking to before revealing sensitive information or entering into a business deal.
- Nonrepudiation is the property of a receiver being able to prove that the sender of some data did in fact send the data even though the sender might later desire to deny ever having sent that data.
- Integrity confirms to you that a message you received was really the one sent and not something that a malicious adversary modified in transit or concocted.

Figure 2-5 Sample Network Security Diagram



2.7.3 DESKTOP KEY SYSTEMS

The age of networked personal computers has brought about a whole new measure of working power to the office environment. This has been accompanied by a great deal of vulnerability. The end user has all the power at their desktop, with the support of a network, to complete their work successfully. This is the apex of the reason for information technology, whether a computer or telecommunications device - so that the human sitting at their workstation can complete their work successfully.

It must always be remembered that the information technology system exists to serve the end user, not the other way around. If security or restrictions are too tight, then the end user can be hampered from completing their work successfully. If, on the other hand, there are not enough measures in place to protect the system's vulnerability, it may suffer damage that would make it difficult, if not impossible, for the end user to complete their work. A balance is crucial in successful systems.

This is the area where the IT system interacts directly with the people who are responsible for the maintenance of the department's essential services. In that sense it is perhaps the most vulnerable point of failure in the network. End users are so dependant upon information technology in our modern age that if their desktop fails, their work progress is often paralyzed.

To manage desktop systems successfully, it is important to know which personnel are involved in what essential services of the department. Often there are a number of people involved in the management of a critical essential service. Example 2.5 demonstrates a way to match persons to essential services. A 'Matching Personnel to Desktop Key Systems' Form is included as Appendix H in Section 3.

Example 2.5: Matching Personnel to Desktop Key Systems

Essential Service	Category	End User (by position)	Workstation Specifications	Crucial Applications	Network Connections
Law Enforcement	*Critical*	*Sherriff's Admin Support*	*IBM ThinkPad*	• *Moving Violations*	• *CIPC* • *Justice Court Transcripts*

2.7.4 SHARED OR GLOBAL KEY SYSTEMS

The Internet has ushered in the age of global sharing of data and networks. Today end users can contribute data from virtually anywhere in the world, communicate online instantly with people in countries in a manner that used to be done by a telephone call or letter, or retrieve software, music or other applications for work enhancement and personal enjoyment.

The downside is that it increases the vulnerability of connected systems exponentially. In order to minimize the risk of disruption to department systems:

- Ensure that all interconnections to global networks are inventoried and that system staff are aware of them;
- Require protection options on internet browsers be maintained and active, e.g.: ms explorer's pop-up window blocker;
- Protect against casual browsing and changes to workstation operating system registry files;
- Install and maintain sufficient virus and intrusion detection software;
- Remain aware of currently active virus and intrusion threats from the internet;
- Restrict downloading of files to only items necessary for work processes;
- Provide end users with sufficient training to understand implications of internet browsing, e.g.: what are "cookies"?; and
- Ensure internet connectivity policies and procedures are clear to end users.

Global connectivity is important in today's modern world of information. Protecting networks in that environment means striking a balance between accessibility and protection.

2.8 SYSTEM RECOVERY EMERGENCY PROCEDURES

The following suggested emergency procedures are designed to assist in system recovery after a system failures. Your system recovery procedures should tie into the overall essential services priorities of your department and links with the Business Continuity Team established early in the process.

One of the primary purposes of an IT Business Continuity Plan is to establish written emergency procedures that the Recovery team can follow to expedite the recovery process. The procedures are in a structured step by step format. This format, during conditions of a system failure, however caused, results in minimal confusion thereby expediting the recovery process. These procedures are dynamic in that as business requirements and environments change so will the emergency procedures. It is imperative each Team Member fully understands his/her role and responsibilities during a system failure and that the emergency procedures are tested on a recurring basis (see Plan Administration). The following emergency procedures have been provided to ensure the individual recovery steps required are followed and serve as a log of the recovery process. Following each step should be a place to initial and indicate the date and time the step was completed as per the following example:

Initials: _____ Date: _____ Time: _____

The emergency procedures have been structured to provide the individual recovery steps required and serve as a log of the recovery process. Following each step is a place to initial and indicate the date and time the step was completed.

The objectives of the emergency procedures are to:

- Minimize injury to personnel;
- Minimize damage to equipment and facilities;
- Achieve a report of injury to personnel and damage assessment within four hours of the interruption; and
- Recover the system and LAN capabilities and functionality within the Significant Time Frames specified.

As the first objective indicates, the safety of every GoA employee in the event of an emergency is of top priority. In an emergency situation where life is threatened or people are in danger of physical harm, they must be directed to immediately leave the facility. Employees are never to place themselves in a dangerous situation or take unnecessary risks.

The emergency procedures to be discussed are follows:

- General
- Recovery Management
- Damage Assessment and Salvage
- Physical Security
- Administration
- Hardware Installation
- Systems, Applications, Network Software
- Communications
- Operations

2.8.1 GENERAL

To report a potential or actual system failure so appropriate action can be taken to minimize injury to GoA personnel and damage to facilities and equipment, use the procedure included in Appendix J.

2.8.2 RECOVERY MANAGEMENT

To decide an escalation plan to be implemented, oversee and coordinate the entire system recovery operation, notify user of estimated time of outage and assist in resolving problems requiring management action, use the procedure included in Appendix K.

2.8.3 DAMAGE ASSESSMENT AND SALVAGE

To assess the damage to the systems and data center within four hours, notify the Management Team of assessment, and coordinate salvage of equipment where possible, use the procedure included in Appendix L.

Under no circumstances should the Damage Assessment and Salvage Team make any public statements regarding the system failure, its cause or its effect on GoA or department operations.

2.8.4 PHYSICAL SECURITY

To ensure the physical security of the disaster site, the alternate site and for files, reports and equipment while in transit and act as liaison with emergency personnel, use the procedure included in Appendix M.

Under no circumstances should the Physical Security Team make any public statements regarding the system failure, its cause or its effect on GoA or department operations.

2.8.5 ADMINISTRATION

To provide administrative support to all System Recovery Teams, including procurement of equipment and supplies, telephones (acquisition and installation), travel and housing arrangements, and other administrative functions not provided by other team members, use the procedure included in Appendix N.

Under no circumstances should the Administration Team make any public statements regarding the system failure, its cause or its effect on GoA or department operations.

2.8.6 HARDWARE INSTALLATION

To plan, design, schedule, install, and verify computing hardware required to provide computer capabilities within the time frame specified. Coordinates with the vendors in support of the equipment, use the procedure included in Appendix O.

Under no circumstances should the Hardware Team make any public statements regarding the system failure, its cause or its effect on GoA or department operations.

2.8.7 SYSTEMS, APPLICATIONS, NETWORK SOFTWARE

To obtain off-site tape backups, restore and test the operating systems, applications and network software needed to provide the capabilities required within the Significant Time Frames specified, use the procedure included in Appendix P.

Under no circumstances should the Systems, Applications, Network Software Team make any public statements regarding the system failure, its cause or its effect on GoA or department operations.

2.8.8 COMMUNICATIONS

To design, install and verify the communications equipment and network cabling, use the procedure included in Appendix Q.

Under no circumstances should the Communications Team make any public statements regarding the system failure, its cause or its effect on GoA or department operations.

2.8.9 OPERATIONS

To provide operating support for the production systems at the backup data center and assist the other recovery teams in establishing operations at the backup site, use the procedure included in Appendix R.

Under no circumstances should the Operations Team make any public statements regarding the system failure, its cause or its effect on GoA or department operations.

2.9 PLAN ADMINISTRATION

Your Business Continuity Information Technology Plan should be a living document and should be directly connected with the department's Business Continuity Plan. Administration procedures are for the purpose of maintaining the IT Business Continuity Plan in a consistent state of readiness. The procedures specify direct Information Technology administrative responsibilities and coordination responsibilities with end users of the data.

These procedures apply to the continued maintenance, testing and training requirements of the IT Business Continuity Plan.

They apply to Information Technology management and user management as a whole to promote awareness of the IT Business Continuity Plan and the need for business disruption preparedness. The procedures also apply to specific functional areas within Information Technology that have direct responsibility for maintaining the plan current and accurate.

The coordination of the IT Business Continuity Plan is the responsibility of the Senior Manager of IT Systems.

2.9.1 MANAGEMENT RESPONSIBILITIES

The function of the Senior Manager of IT Systems and staff is key to maintaining the plan in a consistent state of readiness. The Manager's role is multifaceted. Not only does the Manager assume a lead position in the ongoing maintenance of the plan, but is a member of the IT Business Continuity Plan Team in the event of an IT systems failure.

The areas in which the Manager assumes a lead position and conducts reviews of effectiveness in the plan administration are as follows:

- Distribution of the IT Business Continuity Plan
- Maintenance of the IT Business Impact Analysis
- Training of the IT Business Continuity Plan Team
- Testing of the IT Business Continuity Plan
- Evaluation of the IT Business Continuity Plan Tests
- Review, change and update of the BCIPT

2.9.2 DISTRIBUTION

The Senior Manager of IT Systems and staff should be responsible for the authorized distribution of the plan and the location of each plan copy. The document should be classed as confidential and the authorized distribution list developed on a need-to-know basis. The original and all copies of the IT Business Continuity Plan should be maintained in a secure location.

The concept of IT systems failure planning is to minimize the likelihood of a business disruption ever occurring and further, to minimize impact on department essential services if a business disruption does occur. The IT Business Continuity Plan should reveal in great detail the essence of department recovery strategy, personnel, addresses, locations and inventories which should not be for general publication to nonparticipating employees or outsiders.

Copies of the IT Business Continuity Plan should be assigned a sequential number. The Manager should maintain a log to track the number of copies produced and/or distributed and their location. The original IT Business Continuity Plan should be kept in a secure place to avoid unauthorized duplication or misuse.

Distribution instructions should provide guidance regarding the proper handling and safekeeping of issued plan copies and the requirement for their return upon removal as an IT Business Continuity Plan Team member. IT Business Continuity Plan Team members should be assigned one copy of the Plan. Each Team member should be informed and signify their recognition of the confidential nature of the plan and maintain their copy in a secure location offsite, where it can be easily accessed after business hours. This will allow access to the plan by each Team member in the event access to the department facilities is deemed unsafe or not permitted as a result of a disaster condition. In addition to the Recovery Team members, one copy of the plan should be maintained in a container (number TBD) at the off-site storage facility as well as one copy at the alternate site. Additional copies of the Plan will be assigned to personnel on an as-required basis and as approved by the Chief Information Officer.

2.9.3 MAINTENANCE OF THE BUSINESS IMPACT ANALYSIS

As the department's business and systems environment changes, so does the dependency on the computer systems used to support the department's essential services. Therefore, no less than every two years, the Senior Manager of IT Systems should conduct a Business Impact (Risk) Analysis to update the priority list and Significant Time Frames for the systems recovery process. This analysis will provide insight as to required plan modifications and whether a change in the overall recovery strategy is warranted.

2.9.4 TRAINING AND AWARENESS

The Senior Manager of IT Systems should be responsible for the coordination of training relating to the IT Business Continuity Plan. Wherever possible, training on the IT Business Continuity Plan should be coordinated with department Business Continuity Plan training and awareness sessions. The purpose of IT business continuity training is twofold:

- To train IT Business Continuity Plan Team participants who are required to execute plan segments in the event of a disaster, and
- To train department management and key employees in information technology business continuity and awareness and the need for business disruption recovery planning.

Figure 2-6 - Training and Awareness

Initially, upon the acceptance of the IT Business Continuity Plan, training of department management in business disruption recovery planning benefits and objectives is crucial. An IT Business Continuity Plan must have the continued support from the department's key user management to ensure future effective participation in plan testing and updating. It is not solely the responsibility of the Senior Manager of IT Systems to initiate updates to the IT Business Continuity Plan. End user management must be aware of the basic recovery strategy, how

the plan provides for rapid recovery of their information systems support structure; and how the plan's effectiveness may be compromised without notification to the Senior Manager of IT Systems as their business operations evolve and expand significantly.

It should be the responsibility of each IT Business Continuity Plan Team participant to fully read and comprehend the entire plan, with specific emphasis on their role and responsibilities as part of the Team. On-going training of the Team participants should continue through plan tests and review of the plan contents and updates provided by the Manager.

2.9.5 TESTING AND EXERCISING

There are two methods to validate your IT Business Continuity Plan, testing and exercising.

- Testing refers to the validation of hardware and software performance benchmarks to ensure that IT system viability and integrity is maintained; and
- Exercising refers to the validation of IT system support of department essential services and procedures to be taken by all parties if a business disruption occurs as a result of an IT system failure or in conjunction with an external cause.

There is merit to testing and exercising the IT Business Continuity Plan both as a part of a greater departmental or GoA Business Continuity Plan exercise, or as a stand alone event. The Senior Manager of IT Systems should be responsible for testing of the IT Business Continuity Plan not less than once every year to ensure the viability of the plan and recovery of computing capabilities will be within the Critical Recovery Times established by the Business Impact Analysis. However, special tests and exercises should be given consideration whenever there has been a major revision to the plan or significant changes in the software, hardware or data communications have occurred.

The objectives of exercising the IT Business Continuity Plan would be as follows:

- To determine the effectiveness of the Plan procedures;
- To determine the state of readiness and ability of designated IT Business Continuity Plan Team personnel to perform their assigned recovery responsibilities;
- To determine if sufficient recovery inventories are stored off-site to support the recovery process; and
- To determine if the IT Business Continuity Plan requires modifications or updates to ensure recovery within the Significant Time Frames established and accepted by the end users.

Plan testing can be scheduled when there is less demand for information technology service to end-users since IT personnel and time will be committed to the test process. Costs to conduct such tests and availability of personnel are prime considerations in determining the scope and timing of the test(s). The initial test of the plan will be in the form of a structured walkthrough and should occur within two months of the IT Business Continuity Plan's acceptance. Subsequent tests should be to the extent determined by the Senior Manager of IT Systems that are cost effective and meet the benefits and objectives desired.

The Senior Manager of IT Systems is responsible for making recommendations to department senior management concerning the test scenarios and frequency of tests for the plan. Such recommendations should include sufficient rationale concerning the benefits expected from the test and the specific objectives to be accomplished. Wide latitude would be employed in developing test scenarios. Some considerations in development of the test scenario employed and test frequency could be:

- Significant modifications to the recovery strategy or emergency procedures;
- Inclusion of IT Business Continuity Plan Team members requiring more involvement to sustain familiarity with their respective functions;
- Different severity damage levels to files, documents, materials, and equipment required in support of the recovery process;
- Crucial applications that are new or have not been previously tested;
- Re-testing plan segments which were determined to be deficient in past tests; or
- Additions or changes to IT Business Continuity Plan Team personnel.

Planning for the test would be a two to six week process depending on the complexity of the tests employed and the number of individuals involved. However, without sufficient planning, achievable benefits and objectives from the testing process may never materialize. The steps in planning for the Test in checklist format are:

- Determine Objectives of the Test
- Determine Scope of the Test
- Determine Announced or Unannounced Test
- Determine Personnel Resource Requirements
- Establish Test Date and Duration
- Determine Anticipated Test Costs
- Obtain Test Schedule and Cost Approval
- Schedule Test With Participants
- Schedule Test With Alternative Site
- Schedule Delivery With Off-site Storage
- Make Required Hotel or Travel Arrangements

- Develop Detailed Test Work Plan
- Ensure Recovery Material and Equipment Availability
- Notify Users of Test
- Review Work Plan with Participants

2.9.6 EVALUATIONS

The Senior Manager of IT Systems would be responsible for coordinating the review and analysis of the test results and updating the plan accordingly. A Test Coordination Team should be appointed and headed by the Senior Manager of IT Systems for each test conducted. This team is charged with the following responsibilities:

- To be familiar with the entire plan.
- To understand thoroughly the objectives of the tests to be conducted.
- To organize itself to be able to monitor and observe all the activities of the Recovery Teams involved in the test.
- To inspect and review the results of the test from the point of view of the Information Technology personnel and the users.
- To document their findings related to the strengths and weaknesses observed during the test.

The Recovery and Test Coordination Teams document the test results immediately after the plan test. The Senior Manager of IT Systems reviews the test results with the Recovery and Test Coordination Team during at lessons learned meeting to discuss weaknesses and resolve problem areas. The Manager chairs the meeting and makes changes and updates to the plan accordingly.

2.9.7 PLAN MAINTENANCE

The Senior Manager of IT Systems is responsible for ensuring that the plan is maintained, current and in a state of readiness. The purpose of a plan review is to determine whether updates to the plan or additional training of IT Business Continuity Plan Team personnel is required based on the occurrence of an event or action affecting the plan.

Two primary responsibilities of the Senior Manager of IT Systems will drive revisions to the IT Business Continuity Plan Plan:

1. Updates to the Business Impact Analysis; and
2. Testing of the IT Business Continuity Plan.

However, it is also the responsibility of all department management to initiate a plan review when an event or action affecting the plan has occurred.

2.9.8 CHECKLISTS

The following paragraphs incorporate checklists for department management which could prompt a review and subsequent update of the plan:

- Change in LAN server(s), terminals, or personal computer workstations.
- Change in operating system and utility software programs.
- Change in the design of production systems or files.
- Addition of deletion of a production system.
- Change in the scheme of backing up data or equipment.
- Change in the communications network design.
- Change in personnel assignments or the Information Technology organization.
- Change in off-site storage facilities, location or methods of cycling items.
- Improvements or physical change to the current LAN data center.
- Review of time frames for availability and delivery of replacement computer components.

Corporate Checklist

- Has a new division or department been formed?
- Has a new system been developed for computer processing?
- Has a system for computer processing been discontinued?
- Have individuals within the IT Business Continuity Plan Team been transferred, promoted or terminated?
- Has an internal system been significantly modified to change the basic functions, data flow requirements or accounting requirements?
- Has a department office been opened, moved or closed?
- Are there any user computer equipment inventory changes?

2.10 PERFORMANCE MEASURES

Performance measures relate to two issues within your department's IT Business Continuity Plan:

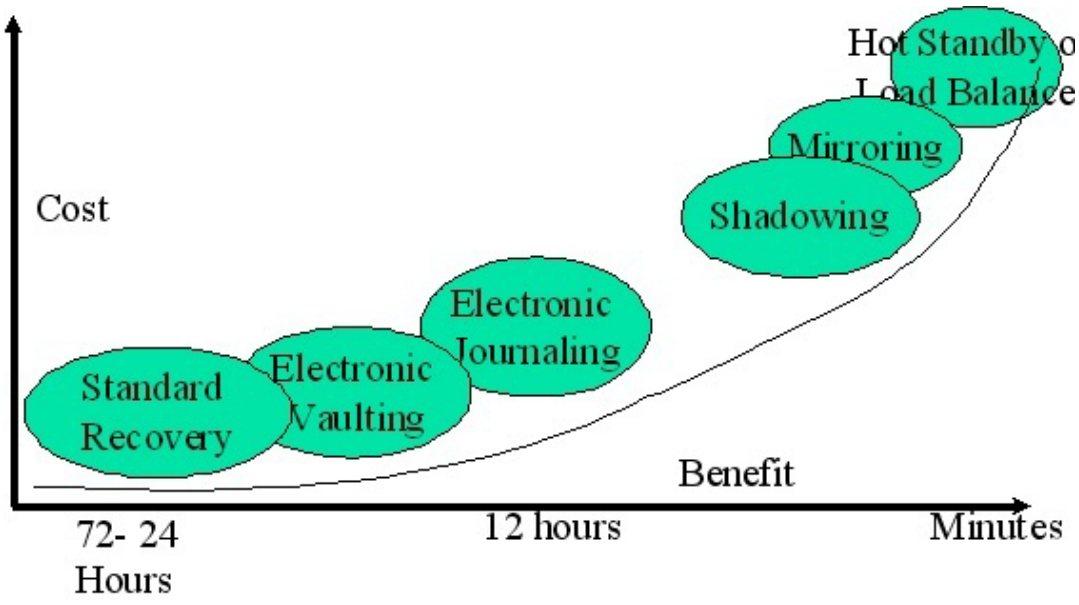
1. The performance of IT systems as they relate to supporting crucial applications and essential services; and
2. The performance of your processes in your IT Business Continuity Plan in support of your IT Systems.

It is important to note that IT business continuity performance measures should not relate to system statistics and data (e.g.: number of packets sent/received on a network).

2.10.1 CRUCIAL APPLICATIONS AND ESSENTIAL SERVICES.

One of the first considerations in the performance measure is the cost/benefit analysis of various methods of prevention, maintenance and recovery for IT systems failure. While it might be nice to have all applications and data backed up on a hot standby platform, the cost may be prohibitive in relation to the benefit received - for example, if the majority of applications do not need to be restored within the 24 hour critical service framework. Figure 2-7 Cost Benefit Ratio illustrates the cost/benefit ratio for a number of popular IT backup and restoration platforms.

Figure 2-7 Cost Benefit Ratio[1]



2.10.2 SYSTEM RELIABILITY

System reliability also needs to be considered as a performance measurement. A "Monthly Measure of System Performance and Reliability" Form, included as Appendix I in Section 3, provides a framework for developing a system reliability measure.

Performance reliability depends upon two measures, failure rate and mean time between failures (MTBF).

1. Failure rate is the frequency with which an engineered system or component fails, expressed in Appendix I in failures per month. Failure rate is usually time dependent, and an intuitive corollary is that both rates change over time versus the expected life cycle of a system. For

[1] With thanks to Deborah Harrop, Workers' Compensation Board of Alberta

example, as a network grows older, the failure rate in its fifth year of service may be many times greater than its failure rate during its first year of service—one simply does not expect to replace a hard drive, system board, or have major transmission problems in a new network. So in the special case when the likelihood of failure remains constant with respect to time failure rate is simply the inverse of the mean time between failure (MTBF), expressed in hours per failure.

2. Mean time between failures (MTBF) is the mean (average) time between failures of a system, and is often attributed to the "useful life" of the device i.e.: not including 'infant mortality' or 'end of life' if the device is not repairable. Calculations of MTBF assume that a system is "renewed", i.e.: fixed, after each failure, and then returned to service immediately after failure. The average time between failing and being returned to service is termed mean down time (MDT) or mean time to repair (MTTR).

SECTION TABLE OF CONTENTS

3. APPENDICES TO IT BUSINESS CONTINUITY PLAN

3.1 PROCESS FORMS SAMPLES

The IT Business Continuity Plan of each department should contain an annex or annexes containing samples of all key forms related to IT business continuity and security. These should include, but are not limited to:

- IT Plan Review Checklist
- Records Classification And Retention Guide
- Records Management Database
- Document Control List
- Document Change Request Form
- Document Change Control Form
- IT Threat / Risk Assessment Report
- IT Security Assessment Checklist
- IT Security Plan
- IT Security Plan Implementation Schedule
- Information Storage Plan
- IT Disaster Recovery Plan
- Access Control Plan
- User Access Control Database
- Access Control Log
- User Account Conventions
- IT Security Audit Report
- IT Nonconformity Report
- IT Security Audit Plan
- IT Incident Report/Response Form

3.2 DATA LOSS PREVENTION MEASURES

It is beyond the scope of this annex to describe all possible accidents in detail and classify them by type. Only the basic cases of data loss will be covered.

3.2.1 DATA LOSS CAUSED BY *SOFTWARE*

While you are editing a document, the program crashes. When you open the file again, all the changes are lost. In the worst case scenario, you cannot open the document at all. There could be multiple reasons behind the crash, such as:

- Faulty device drivers.
- Faulty hardware.
- Corrupt program files.
- Viruses.
- Conflict between some of the running applications.

3.2.2 DATA LOSS CAUSED BY *HARDWARE*

Usually hardware failure is more serious, and the chances of being able to recover data are much smaller. The problem is that unlike in the case of software failure, you can't actually access the data at all (think of a hard disk that doesn't turn on, or of a flash drive with a LED that doesn't blink anymore). Possible causes:

- Faulty hardware (you were one of the "lucky" few customers who purchased a damaged unit).
- Sudden power surges.
- Unstable power source with a great noise level.
- Incorrect unit transportation.
- Negligent use of the device.

Even if hardware can be replaced or fixed, while software can be updated or reinstalled – one problem remains – the lost data cannot be automagically recovered. This leaves you with a single possible approach – *data protection achieved via efficient preventive measures*.

3.2.3 PREVENTING DATA LOSS

Successful recovery from a Data Loss Event generally requires an effective backup strategy. Without a backup strategy, recovery requires reinstallation of programs and regeneration of data. Even with an effective backup strategy, restoring a system to the precise state it was in prior to the *Data Loss Event* is extremely difficult. Some level of compromise between granularity of recoverability and cost is necessary. Furthermore, a *Data Loss Event* may not be immediately apparent. An effective backup strategy must also consider the cost of maintaining the ability to recover lost data for long periods of time.

The most convenient backup system would have duplicate copies of every file and program that were immediately accessible whenever a *Data Loss Event* was noticed. However, in most situations, there is an inverse correlation between the value of a unit of data and the length of time it takes to notice the loss of that data. Taking this into consideration, many backup strategies decrease the granularity of restorability as the time increases since the potential *Data Loss Event*. By this logic, recovery from recent *Data Loss Events* is easier and more complete than recovery from *Data Loss Events* that happened further in the past.

Recovery is also related to the type of *Data Loss Event.* Recovering a single lost file is going to be substantially different than recovering a whole system that was destroyed in a flood. An effective backup regimen will have some proportionality between the magnitude of *Data Loss* and the magnitude of effort required to recover. For example, it should be far easier to restore the single lost file than to recover the whole system destroyed in a flood.

3.2.4 DATA LOSS PREVENTION

It's always daunting to consider deployment of a new security technology, but with the proper preparation Data Loss Prevention (DLP) is less painful to deploy than many other tools. The keys to a successful DLP deployment are setting the right expectations, proper planning during the selection process, and a controlled roll-out.

The most common failure in deploying DLP is failing to set appropriate expectations before and during the selection process. It's important not to jump into DLP before knowing exactly how to use the technology. Do no make a snap purchase to close a single existing problem, or focus on technology-driven expectations that do not reflect business needs. Before you start product evaluations, pull together a team of major stakeholders - including IT, IT security, legal, risk, compliance, HR, and major business units. Determine what data you want to protect, and the degree of protection you would like.

1. Make a prioritized list of the content you want to protect, and map it to a list of desired protective actions. Follow this with a rough outline of workflow so you know which users, technical and non-technical, will need to use the system. This feeds directly into your product selection requirements.

2. Inventory your existing infrastructure and integration requirements. You do not need a detailed assessment of every little device on the network, just an overview of major gateways, data repositories, and endpoint management infrastructure. The combination of your data protection, workflow, and infrastructure integration requirements will form the heart of your product requirements. You will know what kind of content analysis techniques to focus on, whether you will need a point solution (e.g.: an endpoint-only solution) or a complete DLP suite, and what your key workflow requirements are.

3. Stage your DLP roll-out to minimize costly errors. Most DLP customers find they start with passive network monitoring and a basic rules set. They tune the policies until they are happy with the results, then move into active blocking and data-at-rest scanning. The last frontier is typically endpoints, which are deployed on a workgroup basis (where organizations typically use passive alerts, not active blocking). This again lets you tune rules, understand potential business impact, and properly plan for capacity.

Your process, from selection to deployment, has the greatest impact on reducing costs. Give preference to full-suite vendors or to partners whose products are fully integrated. Point solutions force you to create different policies in different systems and then manage incidents on different management consoles that do not necessarily integrate. This situation quickly increases the cost and complexity of a DLP solution.

3.3 SAMPLE SYSTEMS BIA STATEMENT

The purpose of the business impact analysis (BIA) is to help the department identify which business units, operations and processes are important to the continuation of essential services. The BIA will facilitate the identification of how quickly essential business units and/or processes have to return to full operation following a disaster situation. It will delineate the business impact of disaster impact scenarios on the ability to deliver essential services or to support critical services. The BIA will also facilitate the identification of the resources required to resume business operations to a survival level.

Business impacts are identified based on a worst-case scenario that assumes that the physical infrastructure supporting each respective business unit has been destroyed and all records, equipment, etc. are not accessible within 30 days. Recovery assumptions, such as the availability of experienced personnel for recovery, are included in the department's business continuity plan (BCP).

The objectives of the business impact analysis (BIA) are as follows:

1. Estimate the financial impacts for each major department business unit, assuming a worst-case scenario;
2. Estimate the intangible (operational) impacts for each major business unit, assuming a worst-case scenario;
3. Define the estimated number of personnel required for recovery operations; and
4. Identify the department's business unit processes and the estimated recovery time frame for each major business unit.

3.3.1 SCOPE

The scope for the BIA includes the department's essential services and the following business units and shared services:

- Corporate Communications
- Engineering
- Facility Services
- Finance (Including AP and Payroll)
- Human Resources (Including Benefits, Employee Training, Safety/Risk Management)
- Marketing (Including Customer Care, Sales)
- Materials Management
- Network Operations Center (NOC)
- Operations
- Plant Assignment and Dispatch
- Purchasing
- Regulatory Affairs

3.4 INTERNAL CONTACT INFORMATION

The names of all persons within the GoA who need to be notified in the event of an IT systems failure should be listed here. A form is included in Appendix S – "Internal Contact Information by Classification" which provides a method for dividing contacts into classifications. Contact lists should be arranged in priority of calling. Provide a FOIP statement to cover the gathering of personal information.

3.5 EXTERNAL CONTACT INFORMATION

The names of all persons external to the GoA who need to be notified in the event of an IT systems failure should be listed here. This list should include vendors who supply IT services to the department. A form is included in Appendix T – "External Contact Information by Classification" which provides a method for dividing contacts into classifications. Contact lists should be arranged in priority of calling. Provide a FOIP statement to cover the gathering of personal information.

3.6 IT BUSINESS CONTINUITY PLAN TEAM CONTACT INFORMATION

Your IT Business Continuity Plan Team[1] as identified in section 1.6 "IT Business Continuity Plan Organization" should be listed here in priority order of calling. A form is included in Appendix U – "IT Business Continuity Plan Team Contact Information" which provides a method for recording contacts. Contact lists should be arranged in priority of calling. Provide a FOIP statement to cover the gathering of personal information.

[1] Membership on the IT Business Continuity Plan team should consist of at least the persons holding the following positions:
a) Senior Manager of IT Systems
b) Chief Technology Officer Computer Systems
c) Telecommunications Manager
d) Department Business Continuity Officer
e) Information Technology Vendor Representatives
f) Webmaster
g) Web Content Manager(s)
These positions may be described by varying names from department to department. It is important to include those who fill generic roles as outlined above.

3.7 OFF AND ON SITE INVENTORIES

A listing of resources stored on and off site should be provided as an appendix to your IT Business Continuity Plan. A form is included in Appendix V – "Off and On Site Inventory" which provides a method for tracking stored parts and data backup media.

APPENDIX A: RISK ASSESSMENT REPORT FORM

I. Introduction

Describe the system components, elements, users, field site locations (if any) and any other details about the system to be considered in the assessment, including Purpose, Scope of this risk assessment, etc.

II. Risk Assessment Approach

Briefly describe the approach used to conduct the risk assessment, such as:

- The participants (e.g.: risk assessment team members)
- The technique used to gather information (e.g.: the use of tools, questionnaires)
- The development and description of risk scale (e.g.: a 3 x 3, 4 x 4 or 5 x 5 risk-level matrix).

III. System Characterization

Characterize the system, including hardware (e.g.: server, router, switch), software (e.g.: application, operating system, protocol), system interfaces (e.g.: communication link), data and users. Provide connectivity diagram or system input and output flowchart to delineate the scope of this risk assessment effort.

IV. Threat Statement

Compile and list the potential threat-sources and associated threat actions applicable to the system assessed.

V. Risk Assessment Results

- List the observations (vulnerability/threat pairs).

	Each observation must include: • Observation number and brief description of observation (e.g.: Observation 1: User system passwords can be guessed or cracked); • A discussion of the threat-source and vulnerability pair; • Identification of existing mitigating security controls; • Likelihood discussion and evaluation (e.g.: High, Medium or Low likelihood); • Impact analysis discussion and evaluation (e.g.: High, Medium or Low impact); • Risk rating based on the risk-level matrix (e.g.: High, Medium or Low risk level); and • Recommended controls or alternative options for reducing the risk.

VI. Summary

Total the number of observations. Summarize the observations, the associated risk levels, the recommendations and any comments in a table format to facilitate the implementation of recommended controls during the risk mitigation process.

APPENDIX B: IT APPLICATIONS IN SUPPORT OF BIA

INFORMATION TECHNOLOGY BUSINESS IMPACT ANALYSIS

Complete one form each only for applications:

*a) That contain **confidential** information, and/or*

*b) That support **critical** essential services.*

System Name:	
Application Owner/Title:	
ITS Custodian:	
Primary Users:	

System Description:
Database(s), language(s) and release level(s)

Essential Services Supported:

Describe Data Sensitivity (Tables 2-1 and 2-2): [1]

High	Medium	Low

Hardware used: (CPU type)

Network Access (check) ☐ LAN ☐WAN ☐STAND-ALONE
Describe:

Interface(s) to other systems:

How is security access controlled by:

Hardware	
Programs	
Data	

[1] Determine the potential damages to the department of a loss of this IT service using the sensitivity criteria described in Table 2-1.

APPENDIX C: ESSENTIAL SERVICES SUPPORT

Indicate how each essential service is sustained by each support element[1].

Essential Service	Classification (Critical/Vital Necessary/Desired)	Maximum Tolerable Outage	Computer Hardware Support	Computer Software Support	Telecomm Equipment Support

[1] List the hardware, peripherals, software and telecom equipment that is used for each essential service and the key points of support (e.g.: mainframe and financial software supports a cheque run and telecom provides inter-network communication).

APPENDIX D: IT BUSINESS IMPACT ANALYSIS MATRIX

Application	0 - 24 hrs[15]	0 - 72 hrs[1]	0 - 14 days[1]	0 - 14+ days[1]	Recovery Priority[16]	ES Classification

[15] Critical time frames are measured from zero to ensure a standardized priority rating. These columns should reflect he severity of the failure of IT applications on essential service using the scale – **MN** = Minimum Impact; **MO** = Moderate Impact; and **CR** = Critical Impact.
[16] Assign a recovery priority based on the number "1" as highest. This allows for priorization of essential services in the same classification.

APPENDIX E: TIME FRAMES FOR PRE-LOSS MEASURES

MEASURE	DAILY	WEEKLY	MONTHLY	YEARLY	OTHER
System planning					
Current technology					
Preventive maintenance					
System redundancy					
Data backup					

APPENDIX F: STRATEGY SELECTION BASED ON RECOVERY TIME FRAMES OF ESSENTIAL SERVICES

	Expected Outage Time			
Essential Service	**<24hrs**	**>24hrs - <72hrs**	**>72hrs - <2wks**	**>2wks**

APPENDIX G: TABLE OF KEY SYSTEMS AND HARDWARE/SOFTWARE COMPONENTS

Essential Service	Category	System Name / Identity	Hardware Components[17]	Software Applications[2]	Survivability Components[2]

[17] Provide as much detail as possible about individual components.

APPENDIX H: MATCHING PERSONNEL TO DESKTOP KEY SYSTEMS

Essential Service	Category	End User (by position)	Workstation Specifications	Crucial Applications	Network Connections

APPENDIX I: MONTHLY MEASURE OF SYSTEM PERFORMANCE AND RELIABILITY[18]

FOR MONTH OF _____, 20____

	Critical 1	Critical 2	Critical 3	Vital 1	Vital 2	Necessary 1	AVERAGE
Hardware							
Drive							
Server							
I/O Boards							
Peripherals							
Power							
Specialized 1							
Specialized 2							
Software Applications							
Desktop O/S							
Office Suite							
Database							
Financial							
Graphics							
Reporting							
Specialized 1							
Specialized 2							
Network							
Speed							
Router							
Internet							
Gateway							
Server							
Specialized 1							
Specialized 2							
AVERAGE PERFORMANCE AND RELIABILITY PERCENTAGE[19]							

[18] Tracking of "system fault time"[A] is critical in determining patterns of reliability and performance. Use this table to demonstrate percentage of reliability time measured in opposition to down time within a specified time frame. E.g.: If a major outage occurs within a one month period, track the length of time each essential service is affected by each component, then express the difference as a reliability percentage of the measure of the time the system performed satisfactorily.

[19] Percentage figures should be averaged by each row across first, then far right column down.

[A] "System fault time" is considered to be any period of time in which the faulty performance of an IT System adversely affects the performance of time sensitive essential service functions.

APPENDIX J: EMERGENCY PROCEDURE

All protocols to protect life and safety should be developed in accordance with the GoA Facilities Emergency Response Plan (FERP)

IN A LIFE THREATENING SITUATION
IMMEDIATELY LEAVE A DANGEROUS AREA

1. To report an emergency situation dial 9 (to obtain an outside line) and then 911. Report the type of emergency and your name and address.

   Your Office address:

   _____
   _____

2. Immediately notify your Office Administrator, _____ (Extension _____) as to the type of emergency. If the Office Administrator is not available, immediately notify your superior.

3. Notify the Recovery Management Team of the potential or actual system failure or business disruption. The Recovery Management Team may be reached at:

Name	Extension	Phone Numbers
_____	_____	Home: (999) 555-1212
_____	_____	Home: (999) 555-1212
_____	_____	Cellular: (999) 555-1212
_____	_____	Home: (999) 555-1212

APPENDIX K: RECOVERY MANAGEMENT PROCEDURE

A recovery management procedure should tie into existing incident reporting procedure within each department of the GoA.

1. Upon notification of a potential or actual system failure or business disruption, immediately notify the remaining Management Team members and the Damage Assessment and Salvage Team to request that Risk Management and Insurance conduct a damage assessment of the data center facilities.
2. Make an outage assessment based upon the verbal report from the Damage Assessment and Salvage Team.
3. Senior Manager of IT Systems determines where the recovery will be conducted; at the GoA office or the alternate site

   Alternate Site: _____
4. Gain approval for activation of the necessary Recovery Teams and alternate site, if required.
5. Notify other Recovery Team members of the system failure and request they assemble at a designated location for a briefing on the damage assessment and selected escalation plan. The designated location will either be the department offices or the alternate site, depending upon the severity of the system failure.
6. Notify department and division heads on the severity of the system failure and the estimated recovery time.
7. Conduct a briefing with all Recovery team members to apprise of the severity of system failure and determine:
   - Travel and hotel arrangements
   - Equipment acquisitions
   - Equipment repairs
8. Monitor the Recovery Teams that are functioning at the alternate site to resume operations.
9. Assist the Recovery Teams as needed with procurement or any other problems which may require management involvement.
10. The System Manager, reporting to the Senior Manager of IT Systems provides the coordination and assistance to the Recovery Teams in performing their recovery functions.
11. Coordinate and issue any media press releases regarding the system failure as it relates to the GoA and department.

APPENDIX L: DAMAGE ASSESSMENT AND SALVAGE PROCEDURE

1. Assess the requirement for physical security to minimize possible injury to unauthorized persons entering the facility of eliminate the potential for vandalism to GoA or department assets.

2. Utilizing the following checklist as a guideline, survey the systems and data center facilities to assess damage upon notification from the Management Team of the need for damage assessment.

    I. Building
        A. Exterior
        B. Interior
            1. Data Center
                a). Walls
                b). Ceiling
                c). Floor
    II. Environmental/Control
        A. Electrical
            1. UPS
            2. Transformers
            3. Emergency Building
        B. HVAC
            1. Air Handling
            2. Air Conditioning
            3. Water
        C. Fire Suppression
            1. FM-200
            2. Sapphire
            3. Water
    III. Computer Room Contents
        A. Equipment
            1. Servers
            2. External Disk Drives
            3. Tape Backup
            4. Network Cabling
            5. Communications
            6. Terminals
            7. Equipment
        B. Other
            1. Magnetic Tape Media
            2. Spare Parts
            3. Documentation

IV. Department Office Contents
    A. Workstations
    B. Modems
    C. Terminals

The purpose of the above checklist is to provide a guide in the review and assessment of damage following a business disruption to GoA and department facilities, the network and/or the data center facilities. In using the checklist, the Damage Assessment and Salvage Team must consider:

- Is the area safe for employees or vendors to work in?
- Can the equipment under examination function, and if so, at what percent of normal capacity?
- What must be done to recover damaged equipment so that the LAN will be functional?
- How long will it take to repair or replace the damaged equipment so that the LAN will be functional?

3. Based upon damage assessment, determine the estimated time to recover based upon to following guidelines.

   Level I Minimal damage to facility and/or equipment. Estimated time to complete repairs is less than 24 hours.

   Level II Moderate damage to facility and/or equipment. Estimated time to complete repairs is between 24 hours and 7 business days.

   Level III Extensive damage to facility and/or equipment. Estimate time to complete repairs is greater than 7 business days.

4. Identify equipment, documentation or spare parts which are immediately salvageable or in need of repair.

5. Verbally notify the Business Continuity Team of survey, assessment of damage, estimated time to recover from damage and potentially salvageable equipment.

6. Document findings from the survey and damage assessment.

7. Attend the recovery briefing as scheduled by the Senior Manager of IT Systems to apprise Recovery Team members of findings.

8. If the Senior Manager of IT Systems decides recovery will take place at the recovery site and following Risk Management and Insurance and

management approval, salvageable equipment is removed and prepared for transportation to the alternate site or where it can be repaired.

9. A log is prepared and maintained to record all salvageable equipment and its disposition and location.

10. Coordinate with the Administrative Team, vendors and suppliers in restoring or replacing salvageable equipment.

11. Assist in the cleanup of the disaster area in regard to the computer facilities to permit eventual renovation and/or reconstruction.

Under no circumstances should the Damage Assessment and Salvage Team make any public statements regarding the system failure, its cause or its effect on GoA or department operations.

APPENDIX M: PHYSICAL SECURITY PROCEDURE

To ensure the physical security of the computer network and data center, the alternate site and for files, reports and equipment while in transit and act as liaison with emergency personnel, use the following procedure.

1. Upon notification of a system failure or business disruption by the Management Team assemble at the designated site for a briefing on the extent of damages, escalation plan implemented and support required.
2. Establish physical security at the GoA or department facilities to restrict access to the damaged area to those individuals whose functions require their being in the immediate area, such as the Damage Assessment and Salvage Team, insurance company investigators, outsource vendors, and building engineers.

   Considerations in the level of security required are:

   - Is entry into the damaged area safe?
   - Is the damage exclusively to GoA or department facilities?
   - Is there damage to the entire building or has access to the building been restricted by emergency personnel or building management personnel?
   - Are guards required to restrict access to ensure personnel safety or to eliminate possible vandalism or theft of GoA property?
3. Depending upon the extent of the damage to the physical building, coordinate with emergency personnel and building management, access to the building office for those requiring access to the building, such as the Damage Assessment and Salvage Team, insurance company investigators and outsource vendors.

   The Building Management Company contact is:

   _____
   _____
   _____
   _____

   8AM-5PM Phone: (999) 555-1212
   24 Hours Phone: (999) 555-1212
4. Schedule security for all files, reports, and equipment in transit as requested by the Management Team.
5. Assist in any way possible the authorized investigation of the damaged site.

Under no circumstances should the Physical Security Team make any public statements regarding the system failure, its cause or its effect on GoA or department operations.

APPENDIX N: ADMINISTRATION PROCEDURE

1. Upon notification of a system failure or business disruption by the Management Team assemble at the designated site for a briefing on the extent of damages, escalation plan implemented and support required.

2. Coordinate, prepare and submit for authorization to the Management Team procurement requests for equipment, supplies and services required to support the recovery process as requested by the Recovery Team members.

3. Maintain log of all procurements in process and scheduled delivery dates. Notify Recovery Team members of scheduled delivery dates and coordinate with vendors to ensure deliveries or service requests are completed as required.

4. Arrange for travel and lodging required by Recovery Team members or other GoA or department personnel as directed by the Senior Manager of IT Systems.

5. Complete the acquisition and installation of telephone equipment and services as required by the Recovery Team members.

6. Supply required secretarial, filing and other administrative support as required by Recovery Team

Under no circumstances should the Administration Team make any public statements regarding the system failure, its cause or its effect on GoA or department operations.

APPENDIX O: HARDWARE INSTALLATION PROCEDURE

1. Upon notification of a system failure or business disruption by the Management Team assemble at the designated site for a briefing on the extent of damages, escalation plan implemented and support required.

2. Verify with the alternate site the pending occupancy, if occupancy is required, via telephone.

3. Inspect physical space availability at alternate site and notify Software, Communications and Operation Team members.

4. Retrieve the equipment, system and LAN configuration from the storage containers delivered by the off-site storage trustee or vendor.

5. Review the Hardware/Software Inventory list found in the appendix to determine the equipment required.

6. Coordinate with the Damage Assessment and Salvage Team on equipment to obtain an inventory of usable and salvageable equipment.

7. Coordinate with the Administration Team in the procurement of any additional equipment required in the recovery process.

8. Coordinate with the alternate site for installation and connection of 5 temporary terminals to provide access to any mainframe or server for department employees.
   Contact Phone Number _____

9. Coordinate with the alternate site and the Disaster Recovery Team, if activated, for installation and connection of workstations and a server on an ethernet network to support the applications and the various server, if required.

Under no circumstances should the Hardware Team make any public statements regarding the system failure, its cause or its effect on GoA or department operations.

APPENDIX P: SYSTEMS, APPLICATIONS, NETWORK SOFTWARE PROCEDURE

1. Upon notification of a system failure or business disruption by the Management Team assemble at the designated site for a briefing on the extent of damages, escalation plan implemented and support required.

2. Contact the off-site storage facility and request the off-site storage backup tapes, equipment, manuals and documentation.
    a. Backup Medium Storage Container Numbers determined from the pick-up slips located in the back-up log book maintained by the system Administrator. If the back-up log book is not available, have the offsite trustee or vendor look up in their records and deliver the last two containers they picked up.
    b. Documentation/Equipment Storage Container Numbers These numbers will be found in the Appendix - Off-site Inventory.

3. Receive delivery of backup tapes, manuals and documentation at recovery site.

4. Restore the operating system, applications, network software and production data from the backup tapes.

5. Test and verify that the restore completed successfully.

6. Modify configuration of operating and network software to meet configuration.

7. Return backup medium in storage containers to off-site storage.

Under no circumstances should the Systems, Applications, Network Software Team make any public statements regarding the system failure, its cause or its effect on GoA or department operations.

APPENDIX Q: COMMUNICATIONS PROCEDURE

1. Upon notification of a system failure or business disruption by the Management Team assemble at the designated site for a briefing on the extent of damages, escalation plan implemented and support required.

2. Review the Hardware/Software Inventory list found in the appendix to determine the communications and network equipment required.

3. The Communications Team coordinates with the Damage Assessment and Salvage Team on equipment to obtain an inventory of usable and salvageable communications equipment.

4. Coordinate with the Administration Team in procuring communications equipment and telephone lines required in the recovery process.

5. Coordinate with the Administration Team in procuring the necessary network cabling and cabling installation required in the recovery process.

Under no circumstances should the Communications Team make any public statements regarding the system failure, its cause or its effect on GoA or department operations.

APPENDIX R: OPERATIONS PROCEDURE

1. Upon notification of a system failure or business disruption by the Management Team assemble at the designated site for a briefing on the extent of damages, escalation plan implemented and support required.

2. Schedule new pickup point with off-site storage outsourced vendor or trustee.

3. Initialize new tapes as required for recovery process.

4. Complete daily backups of entire system and coordinate with off-site storage vendor to ensure tapes are sent off-site daily.

5. Set-up and operate a sign-in, sign-out procedure for all materials sent to and from the alternate site.

6. Monitor security of the alternate site and the network.

7. Provide production support to users as required.

Under no circumstances should the Operations Team make any public statements regarding the system failure, its cause or its effect on GoA or department operations.

APPENDIX S: INTERNAL CONTACT INFORMATION BY CLASSIFICATION FORM

Name and Position	After Hours Address	After Hours Telephone	Cellular Telephone	Other Number
Senior Management[20]				
Information Technology Staff[21]				
Essential Services Managers[22]				
Facility Staff[23]				
Other GoA[24]				

[20] **Senior Management** should include Deputy Minister, senior official responsible for IT systems, and Communications Director.
[21] **Information Technology Staff** should include all systems analysts, desktop support, network administrators, other specialists and in the event of a network failure the GoA data centre.
[22] **Essential Services Managers** will be determined from the department BCP essential services list as determined by the department BIA. All managers of essential services who may be affected by all or even a portion of the system failure must be notified.
[23] **Facility Staff** may or may not be actual employees of the GoA but should be considered as internal for purposes of system failure notification since the failure may be as a result of a facility failure. Should include building manager, electrical and telecommunications specialists and key facility maintenance workers.
[24] **Other GoA** should include the Business Continuity Section of the Alberta Emergency Management Agency during business hours or the AEMA Duty Manager after hours.

APPENDIX T: EXTERNAL CONTACT INFORMATION BY CLASSIFICATION FORM

Name and Position	After Hours Address	After Hours Telephone	Cellular Telephone	Other Number
Interconnect Suppliers[25]				
Maintenance Contract[26]				
Hardware and Software Vendors[27]				
Data Backup Sites[28]				

[25] **Interconnect Suppliers** should include Internet Service, power company, and communications vendors.
[26] **Maintenance Contract** should include all systems analysts, desktop support, network administrators, and other specialists who provide contractual maintenance support.
[27] **Hardware and Software Vendors** key personnel should listed in priority order.
[28] **Data Backup Sites**. Key contacts having 24 hour control of data backup sites should be listed in priority order.

APPENDIX U: IT BUSINESS CONTINUITY PLAN TEAM CONTACT INFORMATION FORM

Name and Position	After Hours Address	After Hours Telephone	Cellular Telephone	Other Number

APPENDIX V: OFF AND ON SITE INVENTORY FORM

Item Description[29]	Storage Address	On Site[30]	Off Site[31]	Contact Name	Contact Telephone	Storage No.[32]	Data / Media[33]	Parts[34]

[29] If this item relates to continuance of an essential service, please indicate the service in this column.
[30] Indicate with a check mark if this is an “on site” location.
[31] Indicate with a check mark if this is an “off site” location
[32] This could include a number of types of tracking storage numbers, such as barcode, date/time combinations. However it is used to match the item to a central inventory control dataset.
[33] Indicate by a check mark if this is data storage media.
[34] Indicate by a check mark if this is a computer part or repair item.

APPENDIX W: ACKNOWLEDGEMENTS

The following resources were used as study background material for the content of this guide.

- NIST Special Publication 800-30 (US Department of Commerce). *Risk Management Guide for Information Technology Systems*. July 2002. Gary Stoneburner, Alice Goguen1, and Alexis Feringa1.
- NIST Special Publication 800-34 (US Department of Commerce). *Contingency Planning Guide for Information Technology Systems.* June 2002. Marianne Swanson, Amy Wohl, Lucinda Pope, Tim Grance, Joan Hash, and Ray Thomas.
- Alberta Disaster Recovery Planning Guide. *Disaster Recovery Planning Guide for departments and agencies of the Government of Alberta.* January 1996.
- Alberta Student Finance System Disaster Recovery Program. *Alberta Advanced Education and Technology.* May 2007.
- Assumption Management by Robert C. Seacord. *Newsletter of the Software Engineering Institute.* Volume 6 | Number 1 | First Quarter 2003.
- Systems Development Life Cycle Guidance Document. United States Department of Justice. January 2003.
- IT System and Data Sensitivity Classification Ver 01. *Contingency Planning and Business Recovery Program*. Virginia's Community Colleges. February 2007.
- Black Box Testing. Wikipedia Free Documentation License. April 2008.
- Configuration Management. *Defense Acquisition Guidebook.* US Department of Defense. July 2006.
- Data Recovery. Wikipedia Free Documentation License. April 2008.
- Data Recovery. *http://www.hls-systems.com/HLS-Systems/html/data_recovery.htm*. HLS Systems Inc. April 2002.
- Sample Network Security Diagram. Michigan State Police. State of Michigan.
- Kentucky Community and Technical College System Emergency Response/Crisis Management Policy. KCTCS Administrative Policies And Procedures. May 2006.
- Cost Benefit Ratio. *Business Continuity Planning for IT*. Deborah Harrop I.S.P., CBCP, CISSP, CISM. Sr. Manager, IT Infrastructure, Workers' Compensation Board of Alberta. February 2008.
- Hardware Based Security. *The Craft of System Security.* Sean Smith and John Marchesini. November 2007.
- General Information & Process Description. *Business Impact Analysis and Risk Assessment for Information Assets*. Georgia Institute of Technology Department of Internal Auditing. April 2003.

The writer of this guide believes that this list is a complete inventory of background resources that were used to develop the content of this guide. If a reader believes that the list is incomplete or is not fully representative of any portion of the guide, please contact:

Business Continuity Section, Consequence Management
Alberta Emergency Management Agency
14515 - 122 Avenue
Edmonton, Alberta, Canada T5L 2W4