



Government of
Saskatchewan

BUSINESS CONTINUITY PLANNING WORKBOOK 2006

Version 06.1

TABLE OF CONTENTS

1.0	Overview	1
	Protocol During a Disruptive Event	1
2.0	Continuity Planning Development	2
	Establish a Planning Timetable	3
3.0	Identify Mission Critical Functions.....	4
4.0	Complete the Business Impact Analysis	5
	Business Impact Analysis Template	6
5.0	Perform a Threat Risk Assessment	10
	Risk Assessment Template.....	13
	Risk Analysis Matrix	14
6.0	Prioritize Mission Critical Functions	15
	Establish Recovery Time Objectives.....	16
	Prioritize Mission Critical Functions & Set Recovery Time Objectives Template	17
7.0	Developing Business Continuity Strategies	18
	Internal Recovery	18
	Service Degradation	18
	Reciprocal/Cooperative Agreements	18
	Outsourcing	19
8.0	Identify Mission Critical Resource Requirements	19
9.0	Identify Vital Records	19
	Other considerations for vital records:	20
	Vital Records Inventory	21
10.0	Complete an Internal and External Contact List	22
	Contact List – Internal	22
	Contact List - External.....	22
11.0	Write the Plan.....	23
	Sample Business Continuity Plan Table of Contents	23
12.0	Tabletop Exercise.....	25
13.0	Business Continuity Planning Checklist	25

1.0 Overview

To supplement the Government of Saskatchewan Business Continuity Management Planning Guidelines, the Government of Saskatchewan Business Continuity Planning Workbook has been developed to assist business units with creating mission critical specific plans to ensure the restoration of business, operations and departmental support after a disruptive event. The completed plans should form part of the overall **Master Departmental Business Continuity Plan**.

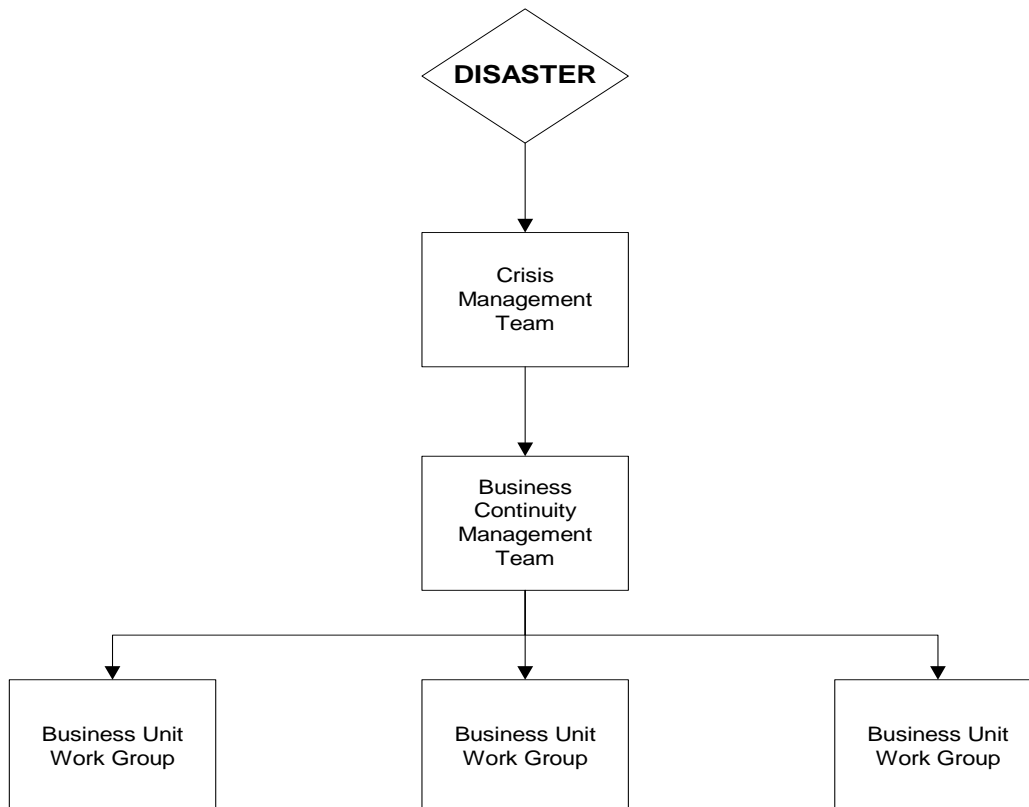
A Business Continuity Plan may outline the following protocol in the event of a disruptive event:

The Crisis Management Team (CMT), which is comprised of upper level management personnel, activates the Business Continuation Plan.

The CMT will then notify the Business Continuity Team (BCT), which is comprised of personnel from key programs. The BCT is responsible for resuming business operations.

The BCT will notify their Business Unit Work Groups. The Work Group will be comprised of personnel involved in supplying the day to day services, programs and operations. The Work Group will carry out their assigned duties as contained in the Business Unit Continuity Plan.

Protocol During a Disruptive Event



2.0 Continuity Planning Development

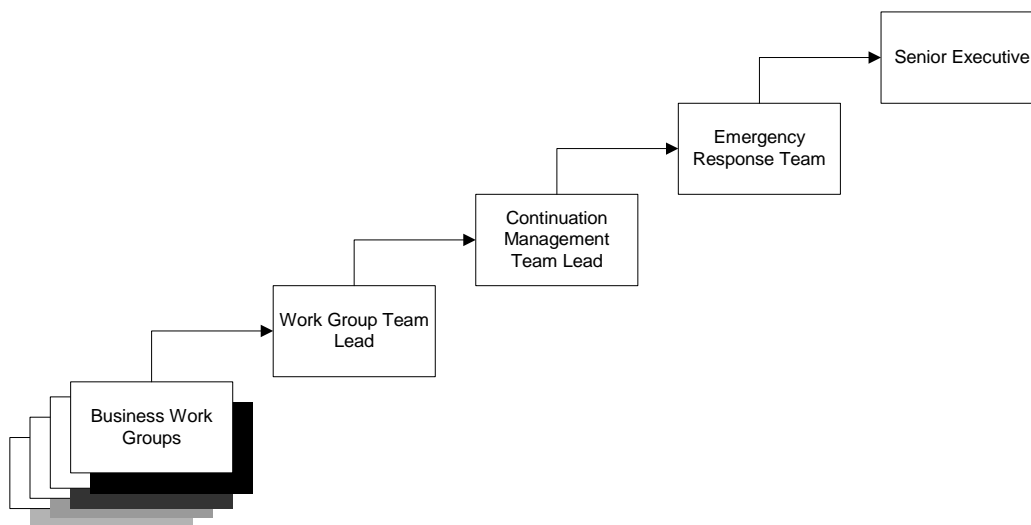
The planning process requires that you ask the following questions:

- ✓ What are your program's mission critical functions?
- ✓ Who is responsible for the provision of those functions?
- ✓ If you were to lose the infrastructure, facilities or personnel that support your mission critical functions, **what will you need and how will you proceed?**

These answers represent the basis for your business continuity plan. The planning phase should include the worst case scenario; a total loss of your facility and tangible property, and should consider the loss of personnel.

The planning templates will assist the work groups in the development of their plans by invoking a logical thought process through each phase. As discussions progress and are recorded, factors to consider will naturally be identified.

The following matrix will provide an opportunity to have the plan reviewed at various corporate levels to ensure all aspects of the continuation of services has been identified. The completed plans will become a protected document that will enable the continuation of business operations.



Establish a Planning Timetable

	Task	Start Date	# of Days to Complete	Completion Date	Person Responsible
1					
2					
3					
4					
5					
6					
7					
8					
9					

3.0 Identify Mission Critical Functions

Identify the mission critical services and functions supplied by your business unit.

	Mission Critical Service/Function	Team Lead	Service Statement (Who – What – Where – When – How – Why the service is supplied?)	Ranking (Critical, Vital Necessary, Desired – outlined in Section 7.1)
1	<u>Example</u> <i>Establishing Communications Centre</i>	<i>Director of Administration</i>	<i>To set up communications at the designated emergency operations centre once a disruptive event has occurred. The communications centre will be used by the Emergency Response Team</i>	<i>Critical</i>
2				
3				
4				
5				
6				
7				
8				

Each business unit will need to identify the mission critical services and functions it delivers.

Assign a Work Group Team Lead who is the most knowledgeable of a particular service or function.

Complete a Service Standard Statement for each service or function. This will identify who, where, when, how and why the service or function is supplied.

4.0 Complete the Business Impact Analysis

A business impact analysis identifies the impacts resulting from disruptions and disaster scenarios that can affect an organization. The goal of a business impact analysis is to identify, categorize and prioritize the critical activities and vital records of an organization. As well, the business impact analysis is an effective management tool to allow the organization to identify interdependencies between different entities in the organization. It also identifies which business processes and assets require the highest level of protection. Finally, the Business Impact Analysis will determine the financial exposures and impacts that an organization faces if a business interruption or disruptive event occurs.

The objectives of a business impact analysis include:

- ✓ Identify critical business functions and operations
- ✓ Identify potential financial exposures and impacts
- ✓ Determine when exposures and impacts begin
- ✓ Determine resources needed (technology, infrastructure, personnel, vendor support)
- ✓ Assess impact(s) of disruption over time
- ✓ Identify interdependencies
- ✓ Determine time criticality of business functions and processes
- ✓ Establish mission critical maximum allowable outage times and recovery time objectives
- ✓ Identify legal and regulatory requirements
- ✓ Determine recovery timeframes and minimum resource requirements

The results of a Business Impact Analysis identify, quantify and qualify the business impacts and their effects on an organization of a loss, interruption or disruption of an organization's critical activities. The technique used for the Business Impact Analysis is a survey format. This survey should be completed by an individual with strong operational and program knowledge of the branch or program area.

Mission critical activities are activities or information that cannot be interrupted or unavailable for several business days without significantly jeopardizing the branch or program area. Moreover, activities that must be completed to ensure regulatory compliance and obligations to the organization, clients or to the citizens of Saskatchewan are classified as mission critical activities.

Critical dependencies are systems, items or devices that a branch or program area relies on in order to carry out its critical activities. Examples of critical dependencies are telephones, fax machines, computers, office space, public access counter, etc.

Resource requirements are the resources needed to ensure that critical activities are delivered to an organization’s clients or to the general public. Each branch or program area must determine the minimum resource requirements for recovery and resumption of critical activities and support systems. Examples of resource requirements are personnel, data sets, etc.

The business impact analysis will determine which processes can be completed manually and which processes have workarounds. Alternate processes and workarounds are key components to the continuity of a branch or program area’s critical activities and processes. It is important to consider the existing procedures and practices, manual interim processes for critical activities and which activities can be deferred or suspended.

Critical: would jeopardize the branch, program area or the government (financially or legally) if this activity was not performed

Important: would impede internal administration or would temporarily cause inconvenience to staff, clients or the public.

Minor: would have no significant impact on operations and services

Business Impact Analysis Template

Business Impact Analysis		
Date:		
Completed by:		
Business Unit:		
Vital Function / Capability Definition	Description	Rating (based on Risk Analysis Matrix – Section 5)
1.0 CRITICALITY ANALYSIS		
1.1 List the main activities/functions conducted/completed by your branch		
1.2 Is there a specific time of day, day of the week, etc. that any functions would be more vulnerable to risk/exposure?		
1.3 Are there written protocols and procedures for each of these activities/functions? Indicate type of documentation and location.		

Business Impact Analysis		
Date:		
Completed by:		
Business Unit:		
Vital Function / Capability Definition	Description	Rating (based on Risk Analysis Matrix – Section 5)
1.4 Can any of the functions listed in Section 1.1 be performed manually or from another location? If yes, please describe.		
1.5 List all computer applications/systems associated with your business unit (including spreadsheets, local databases, etc.)		
2.0 DURATION		
2.1 Would your ability to provide services to your clients and/or the public be immediately impacted by a loss of your system?		
2.2 Could you continue to provide services to the public and/or clients?		
2.3 What is the greatest length of time (hours/days) that the information on the systems can be unavailable?		
3.0 PUBLIC SERVICES		
3.1 Would any services or functions be compromised?		
3.2 If yes, please list assets or services that would be compromised.		
4.0 ADDITIONAL COSTS		
4.1 Give an estimated daily cost if the allowable period of unavailability is exceeded.		
5.0 CASH FLOW & OTHER IMPLICATIONS		
5.1 Is there an impact on cash flow or revenue?		
5.2 If yes, please quantify on a daily basis.		

Business Impact Analysis		
Date:		
Completed by:		
Business Unit:		
Vital Function / Capability Definition	Description	Rating (based on Risk Analysis Matrix – Section 5)
5.3 Are there other financial impacts associated with an outage that have not been addressed?		
5.4 If yes, please describe and quantify.		
6.0 COMMUNICATIONS		
6.1 Would the outage impact your ability to communicate with the public? If yes, please describe.		
6.2 Would the outage impact your ability to communicate with the employees and/or management? If yes, please describe.		
6.3 Would the outage impact your ability to communicate with the clients? If yes, please describe.		
6.4 Would the outage impact your ability to communicate with others (including critical partners?) If yes, please describe.		
7.0 RECORD KEEPING & INFORMATION RETRIEVAL		
7.1 Would an outage have any impact on your record keeping or information retrieval capabilities? If yes, please describe.		
8.0 PUBLIC SAFETY		
8.1 Would an outage have any impact on public safety? If yes, please describe.		
9.0 EMPLOYEE SAFETY		
9.1 Would an outage have any impact on employee safety? If yes, please describe.		

Business Impact Analysis		
Date:		
Completed by:		
Business Unit:		
Vital Function / Capability Definition	Description	Rating (based on Risk Analysis Matrix – Section 5)
10.0 LEGAL LIABILITIES		
10.1 Are there any legal liabilities that might result from an outage? If yes, please describe.		
11.0 REPUTATION, IMAGE & PUBLIC CONFIDENCE		
11.1 Would an outage have a negative impact on the reputation of your branch/division or dep't? If yes, please describe.		
11.2 Would an outage have a negative impact on the public image of your branch, division or department? If yes, please describe.		
11.3 Would an outage have a negative impact on public confidence in your branch, division or department? If yes, please describe.		
12.0 INTERIM SERVICE DELIVERY		
12.1 Could you continue to provide/deliver your services until the operation of your system was restored?		
12.2 If yes, please describe how.		
12.3 If yes, please describe how long you could continue to provide these services in this manner.		

Business Impact Analysis		
Date:		
Completed by:		
Business Unit:		
Vital Function / Capability Definition	Description	Rating (based on Risk Analysis Matrix – Section 5)
13.0 CRITICAL PARTNERS		
13.1 Do you rely on other organization(s) for information or services in order to carry out your responsibilities? If yes, please describe.		
13.2 Does anyone rely on information from your organization in order to provide their services? If yes, please describe.		
14.0 OTHER FACTORS		
13.1 Are there any other factors that would have to be addressed? If yes, please describe.		

5.0 Perform a Threat Risk Assessment

A risk assessment is conducted to determine the internal and external threats that could cause a loss or disruption to your organization, the likelihood of an occurrence and its potential impact.

Losses or disruptions can occur anytime and anywhere and can include injuries and death to employees and the public, property damage, environmental disasters and have significant financial impact. They can be caused by a wide range of risks including human error, technical failure and natural disasters (floods, tornados).

A risk assessment will also identify the controls that are currently in place to reduce the impact of a threat occurring. A control is a process, device or procedure that:

- ✓ Deters a threat from occurring
- ✓ Mitigates impact of a threat
- ✓ Reduces the effect of a threat.

A control will lessen the chance of a threat causing a disruptive event or will mitigate the impact or damage if the disruptive event occurs.

Risk management controls can be divided into three categories:

Physical controls:

- ▶ Fire protection systems (including smoke detectors, sprinkler systems and alarms)
- ▶ Perimeter Security (including card access, commissionaires)
- ▶ Back up generators

Administrative controls:

- ▶ Hiring and termination policies
- ▶ Clean desk policy
- ▶ Policy and procedure manuals
- ▶ Loss of key personnel (review Strike Plans)

Operational Controls:

- ▶ Emergency response plans
- ▶ Standard operating procedures
- ▶ Damage control and spill response, etc
- ▶ IT service interruption procedures

By identifying existing controls within a branch or program area, the effectiveness of these controls can be evaluated and possible exposures can be identified. In evaluating their effectiveness, one must look at their ability to deter or reduce multiple risks.

In addition, one must also determine if the control is being used to its maximum capacity. For example, it is valuable for a branch to say that it has a security system for its office, but it must be determined if the security system is being used effectively.

- ✓ Is the security system armed every night?
- ✓ Are only authorized personnel allowed to set it?
- ✓ Are codes changed on a routine basis?

By reviewing policies and procedures surrounding this control, this allows the control to be used to its maximum potential.

The Risk Assessment will also assist the organization to assess the cost for additional controls to mitigate particular risks. For example, while completing their risk assessment, a licensing unit determines that their highest risk is loss of key staff. By implementing mandatory policy and procedure manuals for each license issuer, the risk will be reduced if key employees are unavailable to perform their job duties.

As a result, a thorough Risk Assessment will provide an effective approach that will serve as the foundation for minimizing the effects of a business interruption or disruptive event.

During the completion of the risk assessment, a crucial step is to identify the existing controls that are in place. Once it has been determined that additional controls need to be explored, it is valuable to select controls with the highest payback. Keep in mind that eliminating a threat may not be possible. However, controls can reduce the effect of a threat.

Controls should be selected with the highest payback based on a cost benefit analysis and should include all costs to purchase/lease, install and maintain controls. Be sure to include the cost for testing and auditing for existing controls. Identifying, improving and recommending additional controls will lower the risks to your organization.

Once the current controls have been identified and additional controls have been recommended, the **TARA** Acronym can be applied to each risk to demonstrate how management has decided to deal with the identified risk. By completing the Threat Risk Assessment, an organization should be able to identify, assess and then explore opportunities to mitigate risk. This is accomplished by transferring the risk, accepting the risk, reducing the risk or avoiding the risk.

Transfer the risk (through insurance or contract)

Accept the risk (where low impact/probability or where no alternative exists)

Reduce the risk (through the introduction of further controls – loss prevention/loss control)

Avoid the risk (by removing the cause or source of the threat)

A risk analysis matrix can also be used to prioritize risks. Any risks that fall into the high and extreme ranking should be dealt with first. For example, a tornado damaging an office building in downtown Regina would fall into the Low/Medium category. The likelihood is once every 100 years (the last tornado to hit downtown Regina was in 1912) or a likelihood of 1. The consequence could be a 5, with a total score of 1 x 5 = 5. A fire damaging a government office building could fall into the High category. The likelihood is once every 10 years for a major loss or a likelihood of 3 and the consequence could be a 5, with a total score of 3 x 5 = 15. Therefore the threat of a fire would be dealt with before the threat of a tornado.

Risk Analysis Matrix

Product (L x C)	RANKING
Score 1-5	Low
Score 6-10	Medium
Score 12-16	High
Score 20-25	Extreme

LIKELIHOOD	CONSEQUENCE				
	1	2	3	4	5
5	Low	Medium	High	Extreme	Extreme
4	Low	Medium	High	High	Extreme
3	Low	Medium	Medium	High	High
2	Low	Low	Medium	Medium	Medium
1	Low	Low	Low	Low	Low

LIKELIHOOD = Probability of the risk event actually occurring.			
Score	Frequency	Approx Probabilities	
1	Improbable, rare, once every 100 years	.00 - .04	
2	Unlikely, once every 10 - 99 years	.05 - .24	
3	Possible, once every 1 - 10 years	.25 - .54	
4	Likely, once a month	.55 - .89	
5	Certain, a few times a month	.90 - 1.00	
CONSEQUENCE = Degree of severity of the consequence.			
Score	Descriptor	Damage & Liability	Operational Effects
1	Insignificant	<ul style="list-style-type: none"> ✓ Loss of power for short time ✓ Loss of asset(s) <\$10,000 	<ul style="list-style-type: none"> ✓ May require some staff overtime
2	Minor	<ul style="list-style-type: none"> ✓ First aid treatment ✓ Loss of asset(s) <\$100K ✓ Disclosure of personal information 	<ul style="list-style-type: none"> ✓ Financial objectives not achieved by 0 - 5% ✓ Schedule delays to minor projects ✓ Some unfavorable media attention ✓ Some unfavorable observations by review groups (Prov. Auditor)
3	Significant	<ul style="list-style-type: none"> ✓ Injury/illness ✓ Environmental damage ✓ Loss of asset(s) \$100K - \$1M 	<ul style="list-style-type: none"> ✓ Disruption of some services ✓ Financial objectives not achieved by 5 - 10% ✓ Schedule delays to major projects ✓ Some loss of client group trust ✓ Negative media attention ✓ Criticism by review agencies (Prov. Auditor)
4	Major	<ul style="list-style-type: none"> ✓ Serious injury/illness ✓ Violation of law (i.e. OHS Act & Regs., Criminal Code) ✓ Disclosure of sensitive information 	<ul style="list-style-type: none"> ✓ Some loss of client group trust ✓ Disruption of numerous services for 1-7 days ✓ Financial objectives not achieved by 10 - 15% ✓ Loss of corporate knowledge ✓ Negative media attention ✓ Criticism by review agencies (Prov. Auditor)
5	Catastrophic	<ul style="list-style-type: none"> ✓ Death or permanent disability ✓ Disclosure of highly sensitive or classified information ✓ Loss of major asset(s) >\$1M ✓ Serious violation of law (i.e. OHS Act & Regs, Criminal Code) ✓ Permanent environmental damage 	<ul style="list-style-type: none"> ✓ Disruption of services >7 days to clients ✓ Cancellation of major project ✓ Financial objectives not achieved by >15% ✓ Loss of key corporate knowledge ✓ Significant loss of client trust ✓ Public outcry for removal of Minister and/ or corporate officials ✓ Media outcry for removal of Minister and/ or corporate officials ✓ Strong criticism by review agencies (Prov. Auditor, etc.)

6.0 Prioritize Mission Critical Functions

These services and functions should be ranked in order of importance. Factors to consider when prioritizing mission critical functions services include:

- ✓ Safety of Personnel
- ✓ Immediate internal and external obligations
- ✓ Legal, regulatory and/ or contractual obligations
- ✓ Dependencies of other departments, service providers or agencies
- ✓ Access to essential information

It may be useful to consider the following questions when prioritizing essential services:

- ✓ What functions would have to be done immediately after a business interruption? What could be postponed?
- ✓ What are your external requirements on a day to day basis? What do you need from outside your business/organization in order to be able to continue to function?
- ✓ What are your immediate internal requirements? Where do they come from?
- ✓ How long can your essential business functions be inoperative?
- ✓ Are there regulatory requirements or penalties that must be considered if you cannot fulfill your obligations due to an unplanned business interruption?
- ✓ What is the financial impact of non-performance of a business function? How significant is this impact? Is it measurable?
- ✓ What are the costs to respond/recover versus the short-term lost revenue?
- ✓ Are other organizations dependent on functions that your business or organization provides?
- ✓ What legal or contractual obligations would arise if the activities were curtailed or shut down?
- ✓ What would be the public relations implications of a curtailment of your activities or a shut-down of your business?
- ✓ Would the safety or security of personnel and property be jeopardized if your operations were interrupted?
- ✓ Which of your essential operations are dependent on computer support? Are there alternative manual operating procedures in place with people who know how to use them? How long these operations could be performed without computer support?
- ✓ List important clients or contacts, external and internal.
- ✓ Identify essential operating information for vital business functions and prepare a checklist of essential records. Maintain copies of essential records off-site.
- ✓ Determine what essential office equipment is required. Specify any special computer hardware, software, databases, networks or other technology.

- ✓ Identify your work in progress. Determine the work flow and business impact if the identified information and work in progress were destroyed and could not be recovered.
- ✓ Identify any work in progress for your business or organization that is being done outside your facility.

Other impact factors that should be considered when determining and prioritizing essential services are:

- ✓ Loss of life
- ✓ Disruption of services to the public
- ✓ Significant damage to or total loss of infrastructure
- ✓ Significant loss of revenue
- ✓ Significant loss of public funds
- ✓ Loss of public confidence
- ✓ Loss of employee confidence
- ✓ Loss of vital records
- ✓ Loss of expertise
- ✓ Disruption of service to other government departments and non-government organizations
- ✓ Mistaken perceptions by the media and the public that could be damaging to the organization and its employees
- ✓ Disruption of obligations to employees

Establish Recovery Time Objectives

The maximum allowable down time of each service or operation will need to be determined. The example below provides a suggested ranking system:

- ✓ **Critical (Priority 1):** Mission critical services that must be provided **immediately** or will **definitely** result in the loss of life, infrastructure destruction, loss of confidence in the Government and significant loss of revenue. These services normally require Continuation within **24 hours** of interruption.
- ✓ **Vital (Priority 2):** Applies to mission critical services that must be provided **within 72 hours** or will **likely** result in loss of life, infrastructure destruction, loss of confidence in the Government, and significant loss of revenue or disproportionate recovery costs.
- ✓ **Necessary (Priority 3):** Those services that must be resumed within **2 weeks** or **could** result in considerable loss, further destruction or disproportionate recovery costs.
- ✓ **Desired (Priority 4):** Those services that **could be delayed for 2 weeks or longer but are required** in order to return to normal operation conditions and alleviate further disruption or disturbance to normal conditions.

Identify Interdependencies:

Information or data may be required from other areas of government or outside sources in order for the business unit to supply the service or function.

Details of this information must be recorded and include what format it is received, area where it is originating, contact person and any other pertinent information.

Prioritize Mission Critical Functions & Set Recovery Time Objectives Template

Critical (within 24 hours)/ Vital (within 72 hours)/ Necessary (within 2 weeks)/ Desired (2 weeks or more)
Priority #:
Essential Service/ Function:
Team Lead:
Team Members:
Recovery Time Objective: (Critical; Vital; Necessary; Desired)
Interdependencies (What information or data is required from other areas in order to perform function):
What format is it received in:
Name & address of area or entity information is received from:
Contact person:
Phone/e-mail address:

7.0 Developing Business Continuity Strategies

The analysis of activities, criticality, seasonality and the consideration of threats and risks will lead us to identify strategies for risk reduction, recovery and risk management.

These may involve some changes to:

- Working practices (e.g. support for home working)
- Succession planning (e.g. training for deputies)
- Investments (e.g. infrastructure, further information technology, desktop computers or laptops)
- Reciprocation or duplication of resources (e.g. information technology or facilities)
- Services (e.g. times of service availability, alternate suppliers, Service Level Agreements, staffing, etc.)

This process is used to determine and guide the selection of alternative business recovery operating strategies for recovery of business and information technologies, within the recovery time objective, while maintaining the organization's critical functions.

It is crucial to develop Business Continuity Strategies that:

- Ensure employee safety
- Protect viability of an organization
- Reduce or mitigate exposures, confusion and chaos
- Position organization to respond to an emergency

Business Continuity Strategies will provide an acceptable level of normalization or level of performance. They must be operationally feasible to carry out during a disruptive event. After determining business requirements and priorities through the Business Impact Analysis, the branch or program area will be able to identify potential alternative strategies.

Internal Recovery

Internal recovery is a feasible solution for a branch or program area that is extremely dependent on a computer application. Purchasing a replication server to have continuous replication of data would provide a branch or program area with the assurance that the data will be protected and most current.

Service Degradation

Service degradation is basically a manner of processing activities in a manual manner. For example, instead of using the computer system to issue a receipt, an individual can issue a manual receipt with a pen and paper, and then the individual could enter this information onto the computer system later.

Reciprocal/Cooperative Agreements

Examine the possibility of transferring critical functions to another branch if possible. Sometimes, "mutual aid" arrangements can be established among areas within a department. For example, make an arrangement with another program area that is located in another city so if they suffer a disruptive event, they will be able to occupy a pre-arranged boardroom, with telephones and computers as a temporary office location.

Outsourcing

Outsourcing is described as turning-over responsibility of some to all of an organization's information systems applications, operations or services to an outside firm or agency. This option is difficult to establish in the government environment. Since the government does not have competition in the services that it provides, it is limited to the fashion in which it can outsource functions. This option is rarely explored.

8.0 Identify Mission Critical Resource Requirements

Develop an inventory of minimal operational requirements needs to be assessed and include:

- ✓ Infrastructure requirements (facilities and work areas /space)
- ✓ Communication equipment requirements
- ✓ Office support equipment, systems, software & furniture (IT)
- ✓ Personnel requirements
- ✓ Any other resource requirements necessary to resume services
- ✓ IT/System related inventory requirements for hardware and software will be developed through IT Support Services. -

9.0 Identify Vital Records

A vital record is data and information required for preserving, continuing or reconstructing the operations of the branch or program area in the event of a business operation or disruptive event.

- ✓ Vital records must be identified and their security classification highlighted.
- ✓ On site and back up storage, format and locations of Vital Records are to be recorded.
- ✓ Persons responsible for the safe keeping of this information are to be identified.

The following provides a guide of what to consider when determining whether a record is vital and examples of what may be considered a vital record:

- ✓ To determine which records are essential, the roles and responsibilities of the organization should be clearly defined.
- ✓ Records should be vital, not merely desirable.
- ✓ Select records as vital also on the basis of ensuring continued delivery of programs and services.
- ✓ Consider what records are required to ensure the ongoing legal, property and other rights of individuals and companies.

- ✓ The criteria for selecting vital records should be established by each business unit at the outset. Consider what information is absolutely required in order to maintain the operations of the organization or to re-build the organization virtually from scratch after a disruptive event.
- ✓ Vital records must be kept current.
- ✓ The “vitalness” of a record may change as work-in progress changes within your business unit.
- ✓ Vital records should be kept in a secure location, geographically separated from your business unit’s office location, in the event that the building and surrounding community is destroyed or rendered inaccessible for an extended period.
- ✓ Choose the most appropriate form of record available in keeping with the need that the information will serve when it is the only copy available (summaries, lists, maps, charts).
- ✓ Records should be completed, concise, clear and easy to understand. If instructions are needed to retrieve or make use of the information contained in records (especially electronic records) those instructions should be included.
- ✓ Some information may be required by other organizations as part of their recovery plan. Consider which records are required and safeguard them as essential records. Similarly consider any information necessary to your operations that are being held by another organization. Make arrangements for the safekeeping of those records.

Other considerations for vital records:

Consider the best method of preserving a vital record: photocopy, storage on computer diskette, tape, etc. Cost effectiveness, accessibility and retrieval mechanisms are other important considerations.

Original records that have been duplicated for vital records purposes should be dated and annotated as having been copied for essential records.

Consider the best place to store your business unit’s vital records (i.e. Departmental office in another city, in a reinforced vault away from your office headquarters, or in commercial storage).

- ✓ Consider how to store your business unit’s vital records: in filing cabinets, in cartons on shelves, special containers and how to keep an inventory of the records and a method of retrieval.
- ✓ Consider the level of physical security and confidentiality required for the records to be stored.
- ✓ Vital records should be tested periodically. If the information they contain is no longer vital, the records should be deleted.
- ✓ Vital records should comprise not more than 10% of the total volume of records held by an organization.
- ✓ A list of who is allowed access to the vital records should be prepared and maintained. The list should be distributed to senior managers and those whose name appears on the list.
- ✓ A master inventory should be created, indicating where each document or piece of information is located.
- ✓ Critical and vital records must have backup copies and be stored off site.

The following checklist is intended as a guide to what may be a vital record:

- ▶ Lists and locations of essential records
- ▶ Lists of key personnel
- ▶ Insurance policies
- ▶ Audit records
- ▶ Bank records
- ▶ Capital assets list
- ▶ Property and land files
- ▶ Details of utility systems (power, water, sewage)
- ▶ Computer programs
- ▶ Court documents
- ▶ Blank forms of various types
- ▶ Personnel records
- ▶ Procedural manuals
- ▶ Financing signing authorities
- ▶ Inventories of equipment and supplies
- ▶ Leases
- ▶ Contracts in force
- ▶ Fixed asset records
- ▶ Contracts and agreements
- ▶ Deeds, blueprints and technical drawings

Vital Records Inventory

Vital Record/Data		Description	Saved Format & Location	Back-up Format & Location	Protection Instructions	Custodian of Information
1	<u>Example</u> <i>Insurance Policy</i>	<i>Legal Contract</i>	<i>Hard copy – SPM Risk Management</i>	<i>Hard copy – Risk Manager’s home Electronic copy – Insurance Broker</i>	<i>Confidential Category B</i>	<i>SPM Risk Manager</i>
2						
3						

10.0 Complete an Internal and External Contact List

Contact List – Internal

This is an example for reference only. Each organization will have different positions identified in its contact list.

Crisis Management / Business Unit Team

Team Position / Name	Home	Work	Cell	Home Address
Team Leader				
Team Alternate Leader				
Communications Team Lead				
HR Team Lead				

Contact List - External

This is an example for reference only. Each organization will have different external suppliers and clients.

Key Client/Critical Supplier

Product / Service	Vendor	Contact Name / Position	Primary Number	Alternate Number	Fax	Email
Insurance Policy	Broker	Account Executive				

11.0 Write the Plan

Sample Business Continuity Plan Table of Contents

Section 1: Plan Overview

Introduction

- 1.2 Emergency Management Program
- 1.3 Purpose of plan
- 1.4 Scope
- 1.5 Objectives
- 1.6 Assumptions
- 1.7 Plan Ownership
- 1.8 Disaster Declaration Processes

Section 2.0: Accountability, Roles, Responsibilities and Authority

- 2.1 Senior Management
- 2.2 Business Continuity Planner
- 2.3 Branch Director or Chair
- 2.4 Business Continuity Teams

Section 3.0: Notification, Invocation and Escalation

- 3.1 Inform Employees
- 3.2 Inform IT Branch, Human Resources, Communications, etc.
- 3.3 Inform Public and Give Other Departments Notice
- 3.4 Arrange Installation of Telephones and Fax (SaskTel)
- 3.5 Configure New or Reconfigure existing Desktop Computers and Install
- 3.6 Order Replacement Computers
- 3.7 Order Replacement Office Equipment and Communications
- 3.8 Contact External Agencies

Section 4.0: Response/Recovery/Restoration Activities

- 4.1 Crisis Response Activities
- 4.2 Damage Assessment Activities
- 4.3 Recovery Activities
- 4.4 Salvage and Cleanup Activities
- 4.5 Restoration Activities

Section 5.0: Implementation of critical activities

- 5.1 Categorization and prioritization of activities
- 5.2 Execution of Critical Activities in a business interruption
- 5.3 Issue licenses
- 5.3 Bank Deposits
- 5.4 Incoming and outgoing documents and mail
- 5.5 Inquiries from public/clients

Section 6.0: Recovery and Resumption Logistics

- 6.1 Personnel
- 6.2 Communications Systems
- 6.3 Computing and Data Systems Recovery
- 6.4 Purchasing

Section 7.0: Critical Business Activities – Recovery Action Plan

- 7.1 Application Failure
- 7.2 Loss of network drives
- 7.3 Power Failure
- 7.4 Access Impossible to Building
- 7.5 Returning to Normal Operations

Section 8.0: Recovery Resource Profile

- 8.1 Applications used by Branch Name
- 8.2 Standard Workstations
- 8.3 Vital documents/records
- 8.4 Operations Documentation Locations
- 8.5 Specialized Equipment

Section 9.0: Plan Maintenance

- 9.1 Business Continuity Plan Testing
- 9.2 Test Team
- 9.3 Annual Review

10. Awareness and Training Activities

- 10.1 Meetings and Seminars
- 10.2 Emergency Team Training
- 10.3 Staff Training

Appendix A – Contacts (Internal and External)

Appendix B – Recovery Site Locations (Infrastructure)

Appendix C – Priority Order of Recovery

Appendix D – Disaster Recovery Plan for IT

Appendix E – Checklists

12.0 Tabletop Exercise

A tabletop exercise is a structured walk-through exercise that simulates an incident in an informal, stress-free environment. This can usually be accomplished in a three to four hour session with the participants gathered in a boardroom or training room. Participants for a tabletop exercise usually include the branch head/director, members of the Business Continuity Management team and the Business Continuity Co-ordinator.

The goal of a tabletop exercise is to educate the responsible individuals on their responsibilities during a business interruption and to identify gaps or inconsistencies in the Plan. A tabletop exercise is a good exercise to start as an initial exercise to test out a Business Continuity Plan.

For more information, please refer to the following document:

Business Continuity Planning Tabletop Exercise White Paper:

<http://www.drj.com/new2dr/toolchest/tabletop.pdf>

13.0 Business Continuity Planning Checklist

Develop Business Continuity Management (BCM) Policy:

- Executive appointed person or team to manage the BCM Program.
- Identify and document the components of the BCM Policy.
- Identify relevant standards, regulations and legislation that must be included in the Policy.
- Develop a draft of a Policy and circulate for consultation.
- Publish and distribute the Business Continuity Management Policy, have a version control system.

Develop BCM Program:

- Define the scope of the continuity management process and program.
- Determine the key approaches to each stage of the BCM life cycle as described in the Guide.
- Research the current state of readiness required by legislation and regulation.
- Report the on the current state of readiness to the Executive, highlight identified gaps.

Develop Business Continuity Plan(s) (BC Plan)

- Appoint an owner for the BC Plan (or each plan for multiple sites).
- Define the objectives and scope for the plan.
- Develop planning process and timetable.
- Decide on the structure, format, components and control of the plan(s).
- Determine which strategies (Organization, Mission Critical, Resource) the plan will document and which will be documented in other plans.
- Determine the circumstances that are beyond the scope of the BC Plan.

Conduct a Business Impact Analysis (BIA):

- Determine scope and terms of reference for the Business Impact Analysis and Risk Assessment.
- Determine what the Mission Critical Activities are.
- Using a worst case scenario determine the timeframe that mission critical activities will suffer both financial and non-financial impacts as a result a disruption.
- Develop Maximum Tolerable Outage criteria for each mission critical activity.
- Identify resource requirements over time to enable each business function within the organization to achieve continuity or resumption of activity within the timeframes established as part of BIA activity. Examples are:
 - ✓ Staff numbers and key skills
 - ✓ Vital Records and data currency (Recovery Point Objective)
 - ✓ Voice and data applications and systems
 - ✓ Infrastructure (cabling and network links)
 - ✓ Facilities (alternative location needs)
 - ✓ Suppliers (intra-organization and/or outsourced providers) and their interdependencies
 - ✓ Constraints (such as contractual issues)
- Present to the Executive to attain approval to move onto continuity strategy design.

Conduct a Risk Assessment:

- List threats to the mission critical processes determined in the BIA.
- Estimate the impact on the organization of the threat using a numerical scoring system.
- Determine the likelihood (probability or frequency) of each threat occurring and weight according to a numerical scoring system.
- Calculate a risk by combining the scores for impact and probability of each threat according to an agreed formula.
- Consider appropriate measures to:
 - ✓ Transfer the risk e.g. through insurance
 - ✓ Accept the risk e.g. where impact / probability are low
 - ✓ Reduce the risk e.g. through the introduction of further controls
 - ✓ Avoid the risk e.g. by removing the cause or source of the threat
- Consider alternative risk management techniques:
 - ✓ Loss prevention – reducing the probability or frequency
 - ✓ Loss reduction – reducing the severity of a loss
 - ✓ Separate the risk or duplicate the information
- Obtain Executive sponsor's approval for the proposed risk management control(s).
- Proceed to development of Organizational, Mission Critical and Resource BCM strategy.

Develop Mission Critical Activity Strategy:

- Prioritize Mission Critical Activities identified in the Business Impact Analysis and Risk Assessment, including their dependencies and any single points of failure.
- Determine the Maximum Tolerable Outage (MTO) using the results from the Business Impact Analysis.
- Determine Recovery Time Objective (RTO) for the process, which should be shorter than the MTO.
- Identify appropriate strategy or strategies for each mission critical process and activity and generate Mission Critical Activity Strategic options.
- Evaluate the cost - benefit for the Mission Critical Activity Strategy options to optimize efficiency, to attain recovery time objectives and to ensure cost effectiveness.
- Provide executive management with a strategic evaluation, which they can assess based on the organization's risk appetite.
- Create Mission Critical Activity Strategy implementation action plans. The Risk Assessment may suggest priority areas for implementation.

Develop Resource Strategy:

- Consolidate the recovery strategy or strategies identified in the previously developed Mission Critical Activity strategic framework.
- Document the resource requirements over time for each mission critical function to achieve continuity or resumption of activity within the timeframes established as part of BIA activity. Examples are:
 - ✓ Staff numbers and key skills
 - ✓ Vital Records and data currency (Recovery Point Objective)
 - ✓ Voice and data applications and systems
 - ✓ Infrastructure (cabling and network links)
 - ✓ Facilities (alternative location needs)
 - ✓ Suppliers (intra-organization and/or outsourced providers) and their interdependencies
 - ✓ Constraints (such as contractual issues)
- Develop and document recovery resources and services strategy to provide for the cost effective restoration of business mission critical processes;
 - a) within their desired Recovery Time (RTO) and Maximum Tolerable Outage (MTO) targets.
 - b) with data recovered to within their Recovery Point Objectives (RPO).
- Identify appropriate strategy or strategies for each Resource and generate Resource Recovery strategic options that will meet the Recovery Time Objectives and are cost effective.
- Provide executive management with a strategy evaluation, which they can validate based on the
- Determine organization's risk appetite.

Write Business Unit Resumption Plan(s):

- Appoint a person to be responsible for development of the plans overall and a representative within each business unit to develop their plan.
- Define the objective and scope of the plans.
- Develop a planning process and timetabled program. Where possible, begin with the plans for the most urgent functions.
- Develop an outline or template plan to encourage standardization of documentation but allow individual variations where this is appropriate. The Business Unit Resumption plan is to structure the response of each business unit to an interruption.
- The Business Unit Resumption Plans provide the Operational Response to the incident of each business unit of the organization. Examples of Business Unit plans are:
 - ✓ A business unit plan to resume its functions within a predefined timescale
 - ✓ An incident response team, sometimes lead by a Facilities branch, who deal with the specific incident and its physical impact (if any)
 - ✓ A Human Resources response to wellness issues of an incident
 - ✓ An IT branch's logistical response to the loss and subsequent resumption of IT services to the business
- Circulate the draft of the plan(s) for consultation, review and challenge within and, where necessary outside, the department.
- Validate the plan through a unit test.
- Consolidate the Business Unit plans and review for consistency.
- Document connections and dependencies with the BC Plan and between Unit plans.

Write Crisis Management Plan:

- Document the responsibilities of the Crisis Management Team and their relationship with other plans. (an example list of responsibilities is in the appendix)
- Develop a Crisis Management Plan that can support the role of the organization's Crisis Management Team during a crisis event
- Develop a Crisis Communications Plan that can manage the media and stakeholder communication during a crisis

Implement and Sustain the Business Continuity Plan(s) (BC Plan)

- Implementation – assess awareness, deliver program, measure results
- Sustainment - Exercising, Audit and Review