DND/CF

Level 1
Business Continuity Plan

TABLE OF CONTENTS

Organization name or acronym

BUSINESS CONTINUITY PLAN

PART 1 – OVERVIEW

Introduction

The Treasury Board Secretariat (TBS) recognized the need to establish a comprehensive process to ensure the continuity of Constitutional Government and critical government of critical services; TBS developed the Business Continuity Planning Program and mandated its implementation through the Government Security Policy.

This (org name) group Business Continuity Plan (BCP) has been developed as part of the Business Continuity Program for the Department of National Defence and Canadian Forces' (DND/CF) and aims to ensure the continued availability of critical services and developed using the Business Impact Analyses that have been developed for each of the Group's critical accountabilities. The focus of this plan is limited to the National Capital Region.

This document contains guidelines and information to ensure the continued availability of essential services and assets of the (??????? Org), and should be implemented in the event of a disruption of normal operations or critical services. It identifies general levels of risk associated with the (Org Name) group controlled services and those outside of its immediate control, and defines the circumstances arise that warrant the implementation of this plan. This is an evergreen document that will be further developed as we proceed with furthering the BCP program within the org name group.

Organization

6. This section should contain:
   - a brief description of the Level 1 organization's vision, mission and accountabilities; and
   - a brief description of the organizational structure and reporting relationships.

Business Impact Analysis

7. This section should include a brief synopsis of the Level 1's BIA, including:
   - any Threat and Risk Assessment (TRA) factors which may apply to this Level 1;
   - a listing of this Level 1's Critical Operations and Services;
   - Internal Dependencies;
   - External dependencies;

- Critical Infrastructure; and
- Gaps and related mitigation plans.

< Note: It may be helpful to display the Critical Operations and Services in tabular form. Example provided below >

ADM(FinCS) < example only CRITCAL OPERATIONS AND SERVICES		
DG Financial Operations	DG Financial Management	DG Corp & Shared Services
1. xxx 2. xxx 3. xxx 4. xxx	1. xxx 2. xxx	1. xxx 2. xxx 3. xxx

Planning and Preparedness

Example: *< The following is offered to provide context to this section >*

8. The Security Operations Standard on Business Continuity Planning describes a best practice BCP program framework as having four essential elements:

- the establishment of a BCP governance structure;
- the conduct of a Business Impact Analysis and Threat and Risk Assessments;
- the development of strategies, plans and arrangements; and
- the maintenance of BCP program readiness.

9. Best practices in the *Governance* area include: the development of a BCP policy instrument to document accountability for the program and set out roles and responsibilities; the assignment of BCP Coordinator(s) to administer the program and Executive Lead(s) accountable for the program; and the creation of committees and working groups to support the development and oversight of the program as well as incident and consequence management.

10. The next element, the BIA identifies what the critical services of an organization are, how resilient they are to hazards as well as identifying operational risks to those services. The BIA is necessary, along with some assessment of threats and risks, for defining mitigation, preparedness and recovery strategies that will form the basis for the organization's risk management strategy. This can be a lengthy process. It requires a lot of discussion within the organization because it deals with 'horizontal' issues. When done well it will result in

better understanding of critical services and what it takes to ensure the survival of those services.

11. The third element of the best practice model includes the development of *strategies, plans and arrangements* to mitigate/respond to and recover from an emergency. Mitigation and management strategies (alternate sites, mirrored systems, hardened facilities, priority dial tone services) are dependent on the risk profile of an organization—its tolerance to risk. Planning focuses on the development of risk-based customized plans. Generally, a BCP details:

- who is responsible for decision making (BCP management and response teams) and for implementation of response measures (key personnel);
- what they are responsible for (critical services/functions, minimum acceptable levels of service) and what they are dependent on (infrastructure, support);
- where these services will be provided from (alternate site);
- who must be informed about the situation (contact lists—employees, clients, corporate services, vendors); and
- how critical services and systems will be recovered (what steps need to be taken to implement/provide service).

12. Plans are expected to deal with the consequences from all hazards that could potentially disrupt the delivery of critical services—whether the event is natural, man-made or technological in its origin. The principle of an 'all-hazards' approach to emergency planning recognizes that the effects of major emergencies are essentially the same despite their causes. This approach optimizes the use of scarce resources through employment of generic planning, response and support methodologies, modified as necessary by particular circumstances.

13. The fourth element of a BCP program is ensuring that the organization *maintains its readiness* by identifying lessons learned from exercises or actual incidents and by building in best practices identified within the organization or employed elsewhere.

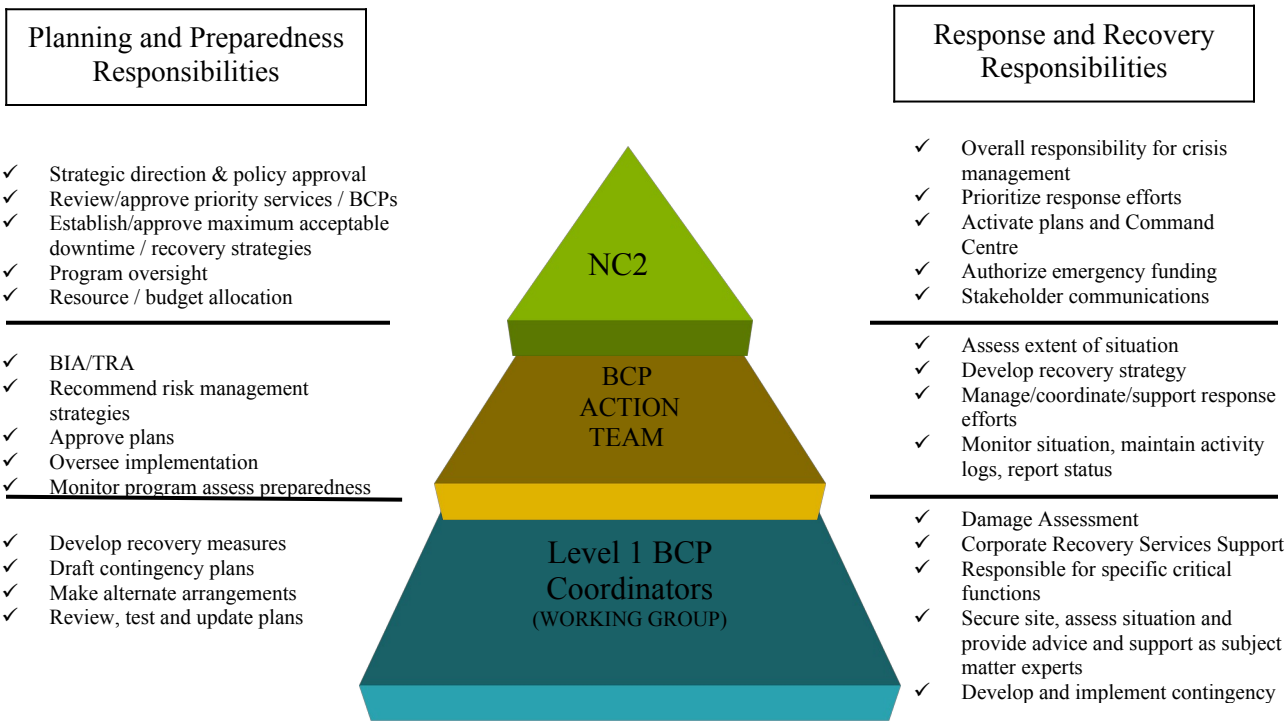
14. Successful BCP programs have formal training and exercise components and are reviewed regularly. In addition, the program elements need to be properly administered. This includes maintenance of the plans and the volatile elements contained therein, on-going review of program assumptions and reporting of program effectiveness issues. Program coordinators and oversight committees are generally responsible for assuring the extent of program readiness and maturity. In addition, internal audits and management reviews are necessary to ensure the program is operating economically, efficiently and effectively.

Roles and Responsibilities Framework

< This section is meant to describe the interrelationships between the various parts of the BCP Program and is provided as background information and is offered to provide context>

15. The diagram below (Figure 1) depicts the key elements of the framework established to manage the two components of DND/CF's business continuity planning – planning and preparedness and response and recovery – and differentiates between the roles and responsibilities for each element. While the diagram shows three tiers of management authority and accountability, each must function in harmony with the others to achieve success. Key in this framework is the links between operations, programming and policy in planning and preparedness, and between decision-making, coordination/support and responders in response and recovery. This Framework describes the various responsible organizational roles and responsibilities for preventing, preparing for, responding to and recovering from any business continuity situation that affects critical services for which DND/CF is accountable.

Figure 1 – DND/CF BCP Framework



Govrnance Structure

16. This section should contain a description of your organization's internal BCP governance structure. As a starting point, the Level 0 BCP governance structure is provided below:

The DND/CF BCP governance structure establishes clear lines of authority, accountability and responsibility. This will ensure that DND/CF is well prepared to respond to a disruption or emergency, thereby facilitating a rapid recovery and restoration of DND/CF operations and services. The DND /CF governance structure includes:

- **Executive Authority.** The VCDS is responsible for the preparation, exercise and maintenance of the DND/CF BCP Program;
- **Senior Management.** The Defence Management Oversight Committee (DMOC) reviews and approves all aspects of the DND/CF BCP Program;
- **Senior Leadership**. Assistant Deputy Minister (ADM) Financial and Corporate Services (Fin CS) and Strategic Joint Staff (SJS) Director of Staff (DOS) provide corporate/CF leadership to the DND/CF BCP Program. ADM(Fin CS)/Director General Corporate and Shared Services (DGCSS) and SJS Director-General Plans (DGP) serve as the co-chairs of the DND/CF BCP Action Team;
- **BCP Coordinator(s).** Senior DND and CF BCP coordinators have been appointed and serve as lead planners for the DND/CF BCP Program;
- **BCP Action Team.** All organizations within DND/CF, as well as key representatives such as the Departmental Security Officer (DSO), are members of the DND/CF BCP Action Team (Director level); and
- **BCP Working Groups.** Functional Level 1 working groups develop and implement the BCP Program within DND/CF.

< Note: this is list should be adapted to the circumstances of your organization >

PART 2 – PLAN IMPLEMENTATION

Crisis Response Procedures

17. This section should contain a description of your organization's crisis response procedures.

Example:
Depending on the nature, extent and severity of the situation, the following steps would be taken: *< Note: this should be tailored to the needs of your organization >*

a. The person on the site of the situation will inform the *<Level 1 Group Principal>* and the Crisis Response Team as required;

b. Following an analysis of the situation, the *<Level 1 Group Principal>* and the Crisis Response Team decide on degree of implementation of the business continuity plan for their respective organization;

c. Each member of the Level 1 organization is responsible for implementing the aspects of the plan under his/her area of responsibility; *<Note: each Level 1 organization is responsible for contacting all employees under his/her immediate supervision>*

d. Depending on the nature, extent and severity of the situation, the initial response will be to advise clients and staff of any prolonged disruption in services concurrently with the re-establishment of the case management systems, file servers, and basic office support facilities at an alternate location.

Also see Annex C – Incident and Consequence Management Guide for more detail on dealing with emergency situations and the consequences.

Response and Recovery Strategies

18. In this section, identify the tasks that are required to support your continuity or recovery of service delivery for each category of service delivered. A separate set of tasks will be required for each identified service.

< The following is offered as an introduction to provide context to this section >

19. Key to the Department's response and recovery from a business continuity disruption is the system of incident management put in place (as part of the planning and preparedness function) to deal with situations affecting critical services.

20. Managing emergencies is complicated and challenging. First and most important is to manage the incident itself and ensure that the health, safety and security of those affected are attended to. Only then will management be concerned with the consequences of the event.

Incident management relates to the measures taken to ensure the health, safety and security of building occupants as well as to the management response to situations that disrupt essential business services. When standard operating procedures in the building emergency plan are implemented but cannot rectify the situation, critical services and systems can be disrupted and the matter must be brought to the attention of management.

21. Consequence management relates to the measures taken to recover from, restore and resume normal business operations after an emergency. The measures taken depend on the type of incident and the nature and severity of its impact on critical services.

22. Another reality is that decision making in emergency situations is dynamic and must be flexible. Managers must consider the events as they unfold and react accordingly (i.e., reprioritize and redirect any operational responses and reallocate resources as necessary). Management direction on the actions to be taken will need to be considered with input from subject matter experts on a case-by-case basis, given that each situation is unique and the measures documented to deal with emergencies are generic. The plans may not exactly fit the situation.

23. The BCP program has a command and control, as well as a communication and coordination structure in place to deal with the incident at hand as well as manage the consequences of the emergency. This structure has been designed to complement the DND/CF BCP. There is also an incident and consequence management regime and a base of operations (emergency operations/command centre) from which to oversee response and recovery efforts.

Example:

Response and Recovery			
#	Activity	Task done by	Remarks
1	Assess nature of emergency	<Name or position> *	In consultation with Team
2	Convene Recovery Management Team / activate Control Centre	*	Primary Site: 1st Alternate: 2nd Alternate:
3	Account for personnel	*	
4	Secure all sensitive information	*	

Response and Recovery			
#	Activity	Task done by	Remarks
5	Advise employees of situation, the telephone number of the Control Centre and disposition of non-essential personnel	*	
etc		*	
< Note: Task descriptions should be sufficiently detailed as to clearly identify the actions required to recover the service or group of service, and identify who is responsible for completing the task. Include any remarks that are appropriate >			

Business Continuity Response Strategies

19. In this section, the following table lists the main situations that could occur and summarises the key elements of the response plan to each situation.

Example

Location Affected	Situation	Focus on:	Risk Management Strategies	Relevant DND Response Plans
Entire National Capital Region	Catastrophic event affecting National Capital and constitutional issues need to be considered	Constitutional Government and deal with issues of national Interest	-	Continuity of Constitutional Government Plan
275 Slater Street	Unable to gain access to offices AND any or all of the infrastructure, applications databases and communications down, regions operating as normal BUT needing IT	Restoring operations – critical services not affected so focus is on operational imperatives IT disaster recovery response – restoring access to systems	• emergency evacuation - health, safety and security of HQ staff • damage assessment and recovery operations • IT disaster recovery • activate alternate site for operations • crisis management • informing stakeholders (e.g. the Minister)	BCP Response Team - Annex A Incident and Consequence Guide – Annex C
	Able to access building BUT any or all of the infrastructure, applications databases and communications down, regions operating as normal BUT needing IT	IT disaster recovery response – restoring access to systems	• IT disaster recovery • informing stakeholders	IT Disaster Recovery Team

Location Affected	Situation	Focus on:	Risk Management Strategies	Relevant DND Response Plans
	Unable to gain access to offices BUT systems working, regions operating as normal,	Restoring operations – no critical services impacted so focus is on operational imperatives	• emergency evacuation - health, safety and security of HQ staff • damage assessment and recovery operations • activate alternate site for operations • crisis management • informing stakeholders (e.g. the Minister)	BCP Response Team - Annex A Incident and Consequence Guide – Annex C
other NDHQ facilities within NCR	Unable to access building BUT systems working, regions operating as normal, lacking HQ support	Restoring operations – no critical services impacted so focus is on operational imperatives Regions manage as normal	• emergency evacuation - health, safety and security of HQ staff • damage assessment and recovery operations • activate alternate site for operations • crisis management • informing stakeholders	BCP Response Team - Annex A Incident and Consequence Guide – Annex B
	Able to access building BUT any or all of the infrastructure, applications databases and communications down, regions operating as normal BUT needing IT	IT disaster recovery response – restoring access to systems Regions manage scheduling and file information locally until able to update systems	• IT disaster recovery • informing stakeholders	IT Disaster Recovery Team

PART 3 – BCP MAINTENANCE, TRAINING AND EXERCISES

Plan Maintenance

20. This section should track changes to the BCP and accompanying annexes. Recommended amendments and updates should be forwarded to your BCP Coordinator. Specifically, maintenance entries should record:

- the conduct of plan reviews and exercises; and
- changes to organizational structures and/or functional responsibilities.

Example:

BUSINESS CONTINUITY PLAN AMENDMENT HISTORY			
Change #	Date	Brief Description and Page Reference	Authorized By
		To be filled in when changes are made to any section	

BCP Training and Exercises

14. This section should describe your Level 1's BCP training and exercise plan.

Annex A

Organization acronym

BCP Implementation

Org name or acronym BCP Response Team		
Name	Position	Responsibilities
* Who are the people in this column?	Level 1 Group Principal Position of person(s) directly related to the responsibilities.>	• assessment of emergency and decision for on level of response required • authority to initiate any required spending, or to request approval to spend additional funds from the VCDS or MDN
*	DGs	• assessment of emergency and decision on level of response required for DND • authority to initiate any required spending
*	BCP L1 Coordinator	• co-ordination of corporate services activities • internal communications •
*	Directors	• Communicate with clients and stake holders
*	L2/L3 BCP Coordinators Local Managers/Supervisors	• co-ordination of onsite BCP activities
*< Note **:** Task descriptions should be sufficiently detailed as to clearly identify the actions required to recover the service or group of service, and identify who is responsible for completing the task. This list should include only operationally critical personnel that have been identified. The above are examples of whom you might include. >*		

<Note: The following tables could be completed for each Level 2 organization that has been identified as having critical operations or services in the level 0 BIA.>

< Note: This information should be derived from the requirements outlined in your BIA >

Resource Requirements	
Item	Description/Numbers
Examples:	
Workspaces/Offices	How many work spaces required?

Resource Requirements	
Item	Description/Numbers
Laptops /with which programs and software	How many?
BlackBerry devices	How many B/B's might be required?
UNCLAS Computers	How many computers? With which programs and software?>
Home telecommunications	How many residences
Printers	How many? Secure LAN, C4 what are your needs?
Photocopier	How many? If any
Secure filing cabinets	How many?
UNCLAS telephone (receive, make local and long distance calls, and voicemail)	How many?
Secure telephone	How many?
UNCLAS fax	How many?
Secure fax	How many?
Offices (including desks and chairs)	How many?
Cubicles (including desks and chairs)	How many?
Filing area	?
Secure conference room	?

<You may wish to add or remove items from the Resource Requirements list>
<If you need it, write it in!>

Mission Critical Systems, Applications and Databases		
Item	Responsibility / Contact	Recovery Time Objective
Examples:		
FMAS	Jane Doe	1-2 days
Example: UNCLAS drives, Outlook, Internet, Intranet (DWAN)	WHO?	What is the maximum allowable down-time?
MASIS		
< Note: This table addresses the organization's mission critical systems necessary to perform essential functions and activities. Organizations must define these systems and address the method of transferring/replicating them at an alternate site. This information should be derived from the requirements outlined in your BIA. >		

Vital Records		
Item	Location	Contact
Examples:		
SOPs		Bob Smith
BCP Plan		
Employee contact lists		
Employee records (necessary for payment of salaries)	Where? Primary? Secondary?	Accountability (Who?)
Beacon registry database and templates for updates	Where?	Accountability
Current financial records (e.g. NIF spreadsheet)	Where?	Accountability
Past financial records (e.g Past NIF spread sheets) (Should be burned onto CD for storage)	Where?	Accountability
Original copies of essential documents (hard copy and CD)	Where?	Accountability
Original copies of essential approval letters (e.g. LMSAR NIF approval, Program Audits		
Copies of NIF templates	Where?	Accountability
?	?	?
< Note: This information should be derived from the requirements outlined in your BIA >		

Alternate Sites	
Primary	Where you are located presently!
Alternate site	Where you would go in the event you have to invoke BCP
Tertiary site	Where you would go if your alternate site was not available
< Note: The defined resource requirements should provide at minimum all requirements for determining your alternate location. This information should be derived from the requirements outlined in your BIA >	

Annex B

Org Acronym

BCP Contact Information

Org Acronym

BCP Response Team Contact List

BCP Response Team Contact List					
Name	Address	Phone (W)	Phone (H)	Phone (C)	Email
*	*	*	*	*	*
*	*	*	*	*	*
*	*	*	*	*	*

< Note: Contact information must be complete and accurate. Events may occur at any time, and will most often require contacting people at home and after hours. The contact list should contain information on every participant involved in the recovery strategy. The above list should include all Response Team that need to be notified >

External Contact List

(This list may need to be updated!!)

This contact list should include the people or organizations, including Essential Suppliers and Contractors (Government and Private Sectors), from whom you will obtain assistance or to whom you will have to provide information in the event of a disruption.

ORGANIZATION NAME	CONTACT NAME AND TITLE	CONTACT NUMBERS	ALTERNATE CONTACT
CRISIS LINE **Director Air Force Employment** **Director General Public Affairs**	**(example) Joe Crisis**	613-555-5555	
OCI PEP Ops Centre			

OCI PEP	**N/A**		
OCI PEP	**N/A**		
CCG	**N/A**		
DFO (CCG)			
Canadian Red Cross Financial Donations	**N/A**		
Canadian Blood Service (Blood Donations)			
257 Slater Commissionare Desk	**N/A**		
275 Slater Building Facilities Contact	**N/A**		
NSS Office emergency Tech Support	**N/A**		
AMEX Travel Arrangements	**N/A**		
Government Sutdown Contact	**N/A**		
RCMP Emergency Duty Officer			
Halifax Joint Rescue Coordination Centre			
Victoria Joint Rescue Coordination Centre			
Trenton Joint Rescue Coordination Centre			
Royal Ottawa Hospital			

* = To be used only by the infrastructure manager department

ANNEX D

Org Name here **STAFF CONTACT NUMBERS**

Toll free in Canada
Sans frais au Canada

Fax machine
Telecopieur

CRISIS LINE: (613) 996-1616

CASCADES TO: (613) 996-

EXECUTIVE DIRECTOR/DIRECTRICE EXÉCUTIVE (DEX)

Name/Nom	Office/Bureau	Home/Domicile	Mobile

FEDERAL COORDINATION/COORDINATION FÉDÉRALE (DFC)

Name/Nom	Office/Bureau	Home/Domicile	Mobile

PROGRAM POLICY AND REVIEW / POLITIQUES DU PROGRAM ET REVUE (DPPR)

Name/Nom	Office/Bureau	Home/Domicile	Mobile

ADMINISTRATION (ADM)

Name/Nom	Office/Bureau	Home/Domicile	Mobile

NON-FEDERAL PROGRAMS/PROGRAMS RetS NON-FÉDÉRAUX (CNF)

Name/Nom	Office/Bureau	Home/Domicile	Mobile

COMMUNICATIONS AND MARKETING/COMMUNICATIONS ET COMERCIALISATION (CCM)

Name/Nom	Office/Bureau	Home/Domicile	Mobile

Annex C

Org Acronym

Incident and Consequence Management Guide

Incident and Consequence Management Guide

Dealing with an emergency situation requires knowing what is going on, how that affects you, then figuring out what to do about it, making that happen and then, letting people know what they need to know. This section provides responders with a checklist / guide for capturing details on the situation and for leading discussions and decision-making.

Understanding the Situation

1. What are we faced with?
   - Nature (what happened?)
   - Extent (how big?)
   - Severity (how bad?)
   - Impact (how does it affect us?)
2. Who is involved? Program/Regions/Other Government Departments/Municipal First Responders?
3. When and how did we find out?
4. What has been done so far?
5. Who else knows? (Public/Media/Unions etc.) Do we know their position/reaction?
6. What are the potential impacts (health, safety, security, services)?
7. How serious is it, is it escalating and what are the consequences?
8. What are others doing?

Incident Management - Dealing with the Situation at Hand

1. Are people hurt? Is there a continuing danger?
2. Are we getting people out of harms way? Are they sheltered?
3. Are trained people providing aid and comfort?
4. How big is the first response (number of fire, police and emergency medical services on-scene) and is it adequate?
5. Who do we have on-site? Have we verified what we know?
6. Do we need to secure the area? Do we need assistance (RCMP, Provincial/ Regional/Local Police)?
7. Can we operate as normal? Reduced levels?
8. Do we need to temporarily close the site?
9. Should we stop (reduce) work?
10. Do families need to be notified? By whom and How?
11. Where do we direct inquiries?

12. Who needs to be notified and what do we tell them? (Families, staff, executive, clients)
13. Who needs to be mobilized and what do we tell them?
14. Do we need to provide assistance?

Dealing with the Consequences - Discuss, Consider, Decide

1. Is the situation a crisis, emergency, business disruption?
2. What measures are needed?
3. What are our obligations here?
4. Do we have enabling legislation or mandate to deal with the issue?
5. Do we have the people, resources, knowledge and abilities to deal with this situation?
6. Do we need assistance/support/advice?
7. Do we need sub-committees to coordinate tasks?
8. Do we have the right people around the table? Are we in contact with them?

Dealing with Business Disruptions

1. What DND services are affected and to what degree?
2. What clients are affected and to what degree?
3. Who in the organization provides that business service?
4. What is the minimum acceptable level of service?
5. What is the recovery time objective? (how quickly do you need to be providing minimal business services and how quickly do you need to be providing full services?)
6. What is needed to do to get the organization back up and providing a minimum acceptable level of business services (action plan / contingency plan)?
7. What is needed in terms of resources (computers, telecommunications, networks, facilities, workstations etc) in order to provide a minimum level of business service?
8. Who in the organization will implement the action plan?
9. What is needed to do to manage the plan?
10. Do you need any staff into the evening or through the night?

External Communications

1. Who will be the spokesperson?
2. What are the messages?
3. What are the other communications needs?
   - News release / media advisory
   - Media lines
   - Press conference

- 1-800 public info line
- Departmental staff
- Fact sheets
- Qs&As
- Briefing Notes
- Question Period briefs

4. Who needs to be notified / updated? How?
   - DM and CDS
   - Level 1 Representative
   - Directors
   - Staff
   - Clients
   - PCO
   - TBS
   - OGDs – Other Government Departments
   - Federal/ other Provinces/Territories/Municipalities
   - Special Interest Groups

Annex D

Org Acronym

BCP Planning Assumptions

Planning Assumptions

< In this annex, include any assumptions that you have made in completing this BCP >

Effective planning requires an appreciation of the risk of a business disruption and the effect it could have on critical services. Because it is difficult to predict the impact of any particular situation, planning is problematic. A number of assumptions need to be made in order to simplify the planning process. The following is a list of the assumptions that were considered in the development of *<insert Level 1 group>* preparedness and response structure:

Example:

1. (Org Acronym) personnel will have access to NDHQ, or be located to an alternate site

2. Sufficient and necessary personnel will be available to perform the (Org acronym) critical operations and services.

Annex E

Org Acronym

Key References

Key References

Examples:

KEY REFERENCES

Policy on Government Security (PGS):
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578

Operational Security Standard – Business Continuity Planning Program:
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/ossbcp-nsopca1_e.asp

DM/CDS BCP Initiating Directive:
http://dmcs-prk.mil.ca/dmcs/FilesO/DMCS70345.PDF

DAOD 1003-0 – Business Continuity Planning:
http://admfincs.mil.ca/admfincs/subjects/daod/1003/0_e.asp

DAOD 1003-1 – Business Continuity Planning Program:
http://admfincs.mil.ca/admfincs/subjects/daod/1003/1_e.asp

DND/CF Business Continuity Plan web site (unclassified):
http://sjs.mil.ca/sites/page-eng.asp?page=1142

DND/CF Business Continuity Plan web site (classified), including:

- the DND/CF Business Impact Analysis (BIA);
- the DND/CF Threat and Risk Assessment (TRA); and
- links to individual Level 1 BIAs

TITAN (CSNI)/Comd-Net Home Page/Corporate/Business Continuity Planning/BIA/DND-CF Level 0/.

National Defence Act:
http://laws.justice.gc.ca/en/N-5/index.html

Organization and Accountability:
http://www.forces.gc.ca/admpol/newsite/home-eng.html

DAOD 9000-1 - CF Succession of Command and Alternate Headquarters
http://admfincs.mil.ca/admfincs/subjects/daod/9001/1_e.asp

DND/CF Pandemic Influenza Plan:
http://sjs.mil.ca/sites/page-eng.asp?page=1416

Operational Security Standard: Management of Information Technology Security

[GoC requirements for IT continuity planning is outlined in sections 12.8 & 18]:
http://publiservice.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/23RECON_e.asp

Policy on Information Management *[Outlines GoC requirements for IM continuity planning]*:
http://publiservice.tbs-sct.gc.ca/pubs_pol/ciopubs/TB_GIH/mgih-grdg_e.asp

Operational Standard for Physical Security (GoC):
http://publiservice.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12329

DND/CF Security Plans and Instructions *[physical security]*:
http://vcds.mil.ca/cfpm/pubs/pol-pubs/intro_e.asp

Defence Administrative Order and Directive 2007-0
[Identifies the authorities responsible for safety in DND/CF]:
http://admfincs.mil.ca/admfincs/subjects/daod/2007/0_e.asp

Directorate of Strategic Readiness:
http://sjs.mil.ca/sites/page-eng.asp?page=917

Library and Archives Canada *[advice on the storage of essential records]*:
http://www.collectionscanada.ca/information-management/index-e.html

Canada Labour Code and the Occupational Health and Safety Regulations:
http://www.tbs-sct.gc.ca/pubs_pol/hrpubs/TBM_119/osh1_e.asp

Canada School of Public Service Business Continuity Planning Course:
http://www.csps-efpc.gc.ca/index-eng.asp

Department of National Defence and Canadian Forces:
http://www.forces.gc.ca/site/home_e.asp

National Search and Rescue Secretariat (NSS):
http://www.nss.gc.ca/

Communications Security Establishment (CSE):
http://www.cse-cst.gc.ca/

Defence Research and Development Canada (DRDC):
http://www.drdc-rddc.gc.ca/

Public Safety Canada (PS CANADA)
http://bcp.ps.gc.ca/