DRAFT V1.3

Level 1
Business Continuity Plan

ADM(IE)

TABLE OF CONTENTS

DRAFT V1.3

ADM(IE)

BUSINESS CONTINUITY PLAN

PART 1 – OVERVIEW

Introduction

1. Canadians rely on their government to provide critical and essential public services at all times—without regard to prevailing operating conditions. Departments are expected to take appropriate risk-management measures that will allow them to manage situations potentially disrupting the delivery of critical services.

2. While it is impossible to prevent the occurrence of business continuity disruptions, planning and preparation can reduce their severity or lessen their impact. The aim of our Business Continuity Planning Program is to ensure the continued availability of the Infrastructure and environment component of Department of National Defence and Canadian Forces' (DND/CF) critical services and assets—services and assets that are essential in fulfilling our mission and mandate.

3. The Government Security Policy (GSP), which came into effect in on February 1, 2002, sets out the requirement for departments to put a business continuity program in place to assure the continued delivery of critical services. The GSP requirements for the continued delivery of services are supported by a Business Continuity Planning (BCP) standard that requires departments to establish a Business Continuity Planning program, consisting of:

- the establishment of a business-continuity-planning governance structure;
- the conduct of a Business Impact Analysis (BIA) to determine mission critical services and systems;
- the conduct of a Threat and Risk Assessment (TRA) to threats and risks to critical services and systems; and
- the development of Business Continuity Plans and arrangements.

4. The DND/CF BCP policy states that:

- CF members and DND employees involved in domestic, continental or international activities will be prepared to deliver critical DND/CF services in the event of any disruption as a result of the application of the departmental BCP Program;
- the purpose of the DND/CF BCP Program is to ensure the continued availability of critical DND/CF services and associated assets; and

- the DND/CF BCP Program provides confidence to employees, stakeholders, clients and Canadians that the department is capable of delivering DND/CF critical services in the face of any hazard to its operations.

Purpose

5. This document contains guidelines and information to provide for the continued availability of essential services and assets of ADM(IE) in the event of a disruption of those operations. It attempts to identify general levels of risk associated with ADM(IE) controlled systems and those outside of its immediate control, and defines responsibilities of key personnel, and the course of action to be followed when circumstances arise that warrant the implementation of this plan.

Organization

6. ADM(IE) is responsible for providing DND and the CF with leadership, policy, planning, advice, oversight, support and services in matters of realty assets, architecture and engineering, the environment, unexploded explosive ordnance, nuclear safety and fire protection, as well as providing leadership of the engineering community. This involves advising and developing, setting and implementing policies and projects in these areas, as well as reporting on how effectively and efficiently these activities are being managed. In addition, ADM(IE) manages legacy sites as well as all infrastructure and environmental issues having significant corporate impacts and exceeding the resources of individual L1s. ADM(IE) is also responsible for the Canadian Forces Housing Agency (CFHA), a special operating agency. In particular, ADM (IE) is responsible for:

- Developing and implementing Departmental policies, plans and procedures for realty assets, fire protection, the environment and nuclear safety programs
- Developing and implementing Department-wide performance measurement systems and reporting requirements for realty assets, the environment and nuclear safety
- Managing corporate real property and the Corporate Environmental Program
- Implementing construction projects
- Developing environmental strategies and policies and promoting compliance with environmental legislation
- Providing advocacy and advice on fire protection, nuclear safety, environmental management and aboriginal affairs
- Establishing the requirements for the Departmental Nuclear Safety Program, including nuclear safety policy
- Overseeing the Canadian Forces Housing Agency

Vision

- ADM(IE)'s vision is be to recognized as the Centre of Expertise for all relevant infrastructure and environment functions in support of CF operations and DND's mandate.

Mission

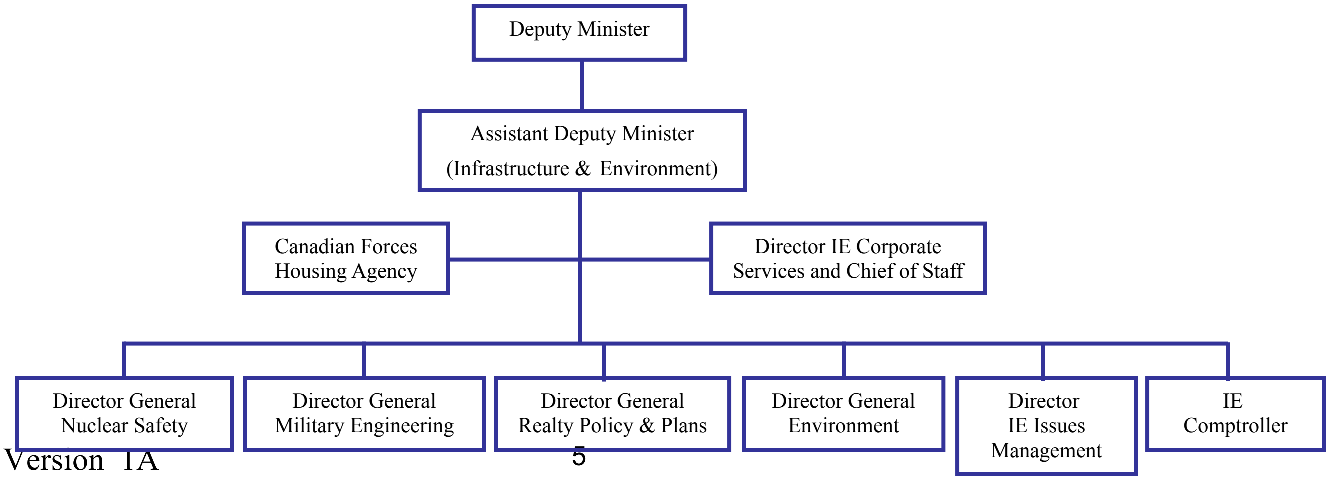
- ADM(IE)'s mandate is to facilitate the delivery of safe, secure, suitable and sustainable infrastructure and environment in support of CF operations and DND's mandate through the provision of relevant and responsive functional direction, guidance and oversight.

7. ADM(IE) carries out his activities with due regard for all areas of functional authority to other L1s in accordance with the Functional Areas Table fm DAOD 1000-0 Corporate Administrative Direction. ADM (IE)'s core accountabilities are summarized in the table below:

ADM (IE) Accountabilities
Life cycle management of national realty assets portfolio
Development and issue of policies and the establishment of standards for the fire protection program and respiratory protection program
Management of national environmental protection and stewardship portfolio
Management of nuclear activity regulations
Oversight of residential accommodation
Supervision of nuclear safety programs
Development and issue of policies and the establishment of engineering and architectural standards for DND/CF infrastructure
Planning and development of the Long Term Capital Plan (Construction) and Capital Investment Plan for infrastructure
Coordination of aboriginal issues (excluding procurement and recruitment)

Table 1 – ADM (IE) Core Accountabilities

8. As depicted below, the direct reports of ADM(IE) include four divisions, three directorates and CFHA:


Deputy Minister
Assistant Deputy Minister
(Infrastructure & Environment)
Canadian Forces Housing Agency
Director IE Corporate Services and Chief of Staff
Director General Nuclear Safety
Director General Military Engineering
Director General Realty Policy & Plans
Director General Environment
Director IE Issues Management
IE Comptroller

- DIECS provides advice and select services to support the delivery of ADM(IE) activities including establishment & application of HR principles; assistance and advice on HR activities and admin support services; corporate changes to ADM(IE) website; linguistic quality and translation services; compliance with the Official Languages Act and implementation of the Ethics program. In addition, DIECS currently functions as the ADM(IE) Chief of Staff

- Director General Nuclear Safety (DGNS). DGNS ensures that DND/CF has an effective nuclear safety program to protect the environment and the health, safety and security of people; is the senior departmental advisor on nuclear technology; ensures that CF operations (domestic and foreign) maintain a high level of operational flexibility with respect to nuclear activities; maintains a high level of safety of personnel and environment with respect to nuclear activities; and develops and enforces DND/CF nuclear safety regulations that are generally consistent with civilian practices.

- Director General Military Engineering (DGME). DGME is responsible for:
  - Construction Project Management
  - Environmental and UXO Project Management
  - Energy Management
  - Engineering Advice (Civil, Mechanical, Electrical, Environmental, and Fire)
  - Architectural Advice
  - Strategic Centre for Fire Protection Policy, Advice and Guidance (CFFM)
- Director General Realty Policy & Plans (DGRPP). DGRPP develops the plans and forecast for delivering all Realty support to the Canadian Forces; reports on the progress and performance of this support; and advises on how to deliver this support within funding limits and the limits of Government policies and laws regarding realty.

- Director General Environment (DGE). DGE is responsible for a wide range of policies and programs dealing with the environment. This includes contaminated sites, climate change, pollution prevention, environmental engineering, sustainable development, environmental assessment, urban and rural forestry, pesticide management and species at risk.

- Director Infrastucture & Environment Issues Management (DIEIM). DIEIM is the lead for responses to complex issues and 'hot' files relating to infrastructure and environment. These issues are often multi-player and multi-jurisdictional. DIEIM is responsible for delivering the coordination and sound judgment required to identify, manage, and mitigate risk, and lead solutions within and across DND and with OGDs.

- Infrastructure & Environment Comptroller (IE Compt). IE Compt is accountable for ensuring continuous improvement of financial business management practices, financial integrity, responsible spending and accountability through the development, implementation and oversight of sound internal controls, plans, policies and procedures, and the delivery of timely and accurate accounting and reporting, and the requisite financial services that effectively and efficiently support the objectives of ADM(IE). IE Compt provides financial management and accrual accounting advice and services.

- The Canadian Forces Housing Agency's (CFHA) mandate is to operate and maintain the portfolio of approximately 14,000 residential housing units at Canadian Forces bases and wings across Canada, including allocating housing to Canadian Forces members and their families, carrying out maintenance and repairs, administering the rent system and managing the housing assets on behalf of the Department of National Defence.

Business Impact Analysis

9. The DND/CF Threat and Risk Assessment (TRA) identified a wide variety of events that could affect DND/CF operations and services. These events can be categorized as resulting in:

a. a loss of staff, e.g. due to a Pandemic Influenza;

b. a loss or disruption of services, e.g. electricity or network services; and/or

c. a loss or disruption to facilities, e.g. fire or physical attack.

10. The following Threat and Risk Assessment (TRA) factors extracted fm the Level 0 Business Impact Analysis are applicable to ADM(IE).

THREAT RISK ASSESSMENT		
Threat	**Probability of Occurrence**	**Remarks**
Loss of Staff		
Strike	High	A strike could impact the response time of services. It could also result in restricted access to and/or the loss of facilities for a period of time. In the case of a general strike, if personnel cannot cross the picket line, it may impact on the services provided by ADMIE. Executife and military staff will be capable of conducting critical operations.
Fire/Bomb Threat/Hazardous Materials	Medium	In the event of one of these emergencies, it could result in potentially some loss of staff (personnel could be injured or killed). The facility would have to be evacuated and the type and impact of the incident would determine when personnel could return to their

		place of work
Natural Disaster	Medium	Winter storms, such as the Ice Storm, can result in the loss of staff for short periods of time ranging from hours to a matter of days. Employees that live outside of the urban area will be most affected. For ADMIE, this will be low impact as less than 5% of personnel live fm outside of the urban area.
Pandemic Influenza	Low	It is estimated that up to 30% of staff could be infected with the influenza and/or be quarantined when family members are infected. Travel will be limited in order to prevent the spread of the influenza. This could result in the short term and/or long term loss of staff that possess critical skill sets and knowledge for the organization.
Losss &/or Disruption of Services		
Interruptions to the supply of public utilities (power, water)	High	Major power loss which last for periods to several days may affect critical services and systems, which require backup power, supply to ensure a minimum level of service.
Interruptions to telecommunications services	High	The probability of a short interruption to local telecommunications services is high, however, it is assumed that commercial carriers has sufficient redundancy to re-establish backbone services and telephone services within a short time period (less than a day). Wireless services do not have the same level of redundancy and are highly vulnerable to power outages. Personnel will have to use the communication services, which will be available to continue their work.
Interruptions to network services (loss of utilities, sabotage, fire/water damage)	High	There is a high probability of local outages of network services that could impact on limited number of users and sites for a limited amount of time. Due to redundancy and backup capabilities, it is anticipated that network services will be restored within few hours to few days.
Fire/Water Damage	Medium	Fire could occur at a specific facility, or the water sprinklers could be activated in a facility. Either way, the facility damage could result in temporary loss of the facility. The services provided by ADMIE could be unavailable for a short period of time; critical services would continue to be provided from an alternative location.
Bomb Threat/Hazardous Materials	Medium	In the event of a bomb threat or hazardous materials incidents, the facility would have to be evacuated, inspected and if no damage or safety risk exists after the inspection, then the disruption to service availability could be in the order of hours. If a full-blown incident occurs, it could result in the extended loss of the facilities and disruption of services for a long period of time; critical IE services would continue to be provided from an alternative location.

Natural Disaster (storm, earthquake, etc.)	Medium	The likelihood of minor damage to roofs, windows and building facilities is medium, depending of the incident. A severe incident such as en earthquake or heavy snow accumulation on the roof could cause significant damage that could leave the facility unusable for an extended period of time. IE critical services would continue from an alternative location.
Man-made causes (i.e. Strike, Sabotage/Terrorist Attack)	Low-Medium	While the probability of a man-made cause for loss and/or disruption of facilities is low to medium, the most likely cause is limitation of access due to a strike for a short periods of time. Damage from sabotage is more likely to occur to Information Management Systems, with the penetration of firewalls and could result in lost data, loss of integrity, data compromise or loss of data availability. Depending on the severity of the attack against the systems, operations and corporate services could be affected.

Table 2 – ADM (IE) Threat Risk Analysis

11. Following is a listing of ADM(IE)'s Critical Operations and Services

ADM(IE) CRITICAL OPERATIONS AND SERVICES								
Critical Ops and Services	COS/DIECS	DGME	DGRPP	DGNS	DGE	DIEIM	IE Compt	CFHA
Corporate Support and guidance to the Minister	X	X	X	X	X	X	X	X
Provide advice and support on policies and standards for the fire protection program and respiratory protection program		X						
Provide advice and support on policies and on engineering and architectural standards for DND/CF infrastructure		X						
Military Family Accommodations Support Services								X
Management of national environmental protection and stewardship portfolio					X			
Supervision of nuclear safety programs				X				

Table 3 – ADM(IE)'s Critical Operations and Services

12. The following are the Internal Dependencies identified in the ADM(IE) BIA

a. DWAN Accessibility
b. Availability of Blackberry service
c. MP (NIS)
d. All L1 BCP POC
e. FMAS/TITAN
f. Secure Fax
g. IM/IT support
h. Telephone service for providing emergency repair and services support delivery (health and safety issues) to the MQ occupant
i. Emergency after hours service provided thru the Commissionaire
j. CFHA Primary Servers
k. Housing Agency Management Information System (HAMIS) Financial
l. HAMIS Housing
m. SMS Salary management system
n. Single safe to ensure financial instruments are well secured
o. Telephone (landline) with voicemail
p. Digital and analog Cell phones
q. All groups and commands with radioactive material
r. Nuclear Safety Information Control System (NSICS)
s. Manuals - SOPs for DGNS Technical Assistance Team (TAT)

13. The following are the External Dependencies identified in the ADM(IE) BIA

t. Maintenance and Service delivery fm various contractors throughout 26 sites across Canada
u. Contracting Authorities (PWGSC) to maintain capability to procure goods and services
v. On safety side, need response fm fire and ambulance in case of physical infrastructure damage, especially MQs
w. Services such as electricity, water and telecommunications (phones/wireless devices)

Planning and Preparedness

14. 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.

15. 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.

16. 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.

17. 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).

18. 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.

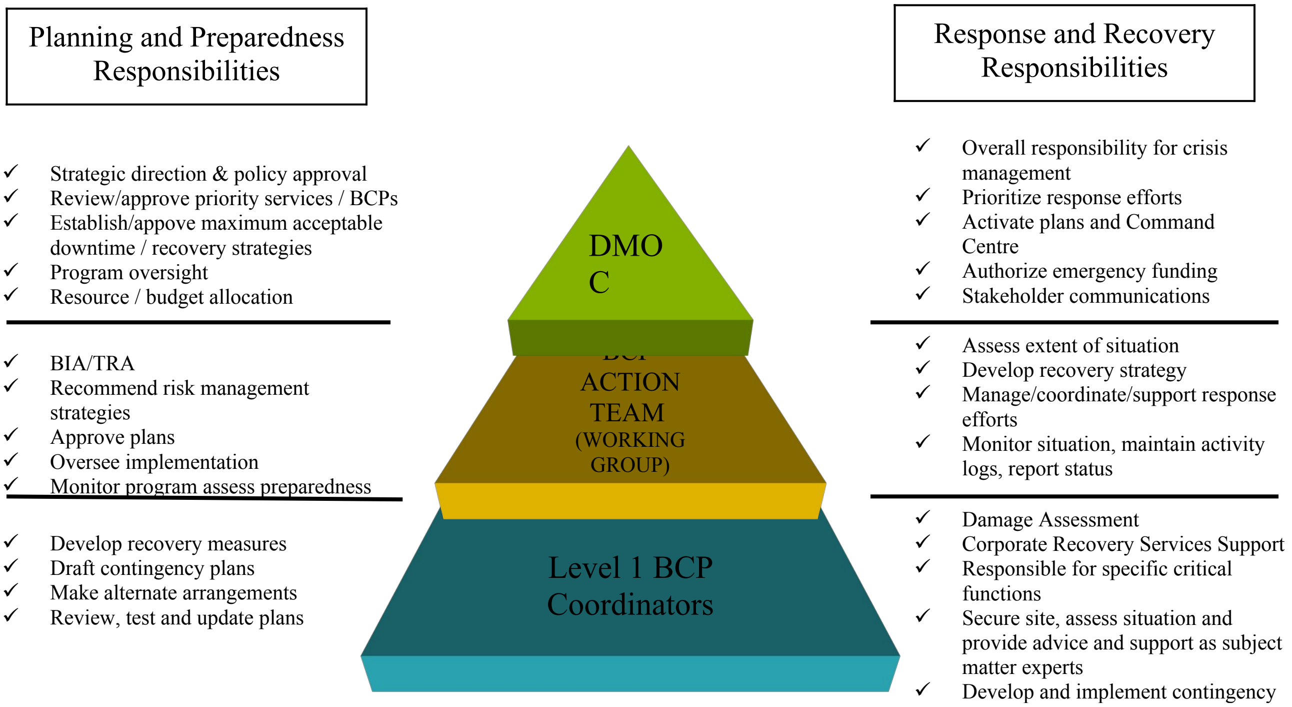
19. The fourth element of a BCP program is ensuring that the organization *maintains its readiness* by identifying lessons learned from exercises or actual incidents and by building in best practices identified within the organization or employed elsewhere.

20. 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

21. 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



Planning and Preparedness Responsibilities

- ✓ Strategic direction & policy approval
- ✓ Review/approve priority services / BCPs
- ✓ Establish/appove maximum acceptable downtime / recovery strategies
- ✓ Program oversight
- ✓ Resource / budget allocation

- ✓ BIA/TRA
- ✓ Recommend risk management strategies
- ✓ Approve plans
- ✓ Oversee implementation
- ✓ Monitor program assess preparedness

- ✓ Develop recovery measures
- ✓ Draft contingency plans
- ✓ Make alternate arrangements
- ✓ Review, test and update plans

Response and Recovery Responsibilities

- ✓ Overall responsibility for crisis management
- ✓ Prioritize response efforts
- ✓ Activate plans and Command Centre
- ✓ Authorize emergency funding
- ✓ Stakeholder communications

- ✓ Assess extent of situation
- ✓ Develop recovery strategy
- ✓ Manage/coordinate/support response efforts
- ✓ Monitor situation, maintain activity logs, report status

- ✓ Damage Assessment
- ✓ Corporate Recovery Services Support
- ✓ Responsible for specific critical functions
- ✓ Secure site, assess situation and provide advice and support as subject matter experts
- ✓ Develop and implement contingency

Governance Structure

22. The ADM(IE) 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 ADM(IE) governance structure includes:

- **Executive Authority.** The ADM(IE)/COS is responsible for the preparation, exercise and maintenance of the ADM(IE)'s BCP Program;

- **Senior Management.** The ADM(IE) Senior Group reviews and approves all aspects of the ADM(IE)'s BCP Program;

- **Senior Leadership**. ADM(IE)/COS provide ADM(IE) Group leadership to the ADM(IE) BCP Program;

- **BCP Coordinator(s).** ADM(IE)/COS and DIECS 2 are the ADM(IE) BCP representative and serve as lead planners for the ADM(IE) Program; and

- **BCP Action Team.** All four divisions, three directorates and CFHA within ADM(IE) are members of the ADM(IE) BCP Action Team (Director level);

PART 2 – PLAN IMPLEMENTATION

Crisis Response Procedures

23. Depending on the nature, extent and severity of the situation, the following steps would be taken:

a. The person on the site of the situation will inform the ADM(IE and/or ADM(IE)/COS;

b. Following an analysis of the situation, the ADM(IE) and/or ADM(IE)/COS and in consultation with the IE Management Team decide on degree of implementation of the business continuity plan for the organization;

c. Each L2 member of ADM(IE) is responsible for implementing the aspects of the plan under his/her area of responsibility as directed by ADM(IE);

d. Depending on the nature, extent and severity of the situation, the initial response will be to advise 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

24. 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.

25. 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.

26. 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.

27. 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.

28. 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.

29. The BCP program therefore has a command, control, 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.

Response and Recovery			
#	Activity	Task done by	Remarks
1	Assess nature of emergency	ADM(IE)	In consultation with ADMIE Management Team
2	Convene Crisis Response Team and activate IE crisis Office	ADM(IE)	Primary Site: Pearkes 1st Alternate: Standard Life 2nd Alternate: Thurnston
3	Account for personnel	All supervisors	
4	Advise employees of situation, the telephone number of the IE Crisis Centre and disposition of non-essential personnel	IE Management Team	

Table 4 – ADM (IE) Response and Recovery

Business Continuity Response Strategies

30. 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.

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
Pearkes Building NDHQ	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)	ADM(IE) Crisis 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	ADM(IE) Crisis Response Team - Annex A IT Disaster Recovery Team
	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)	ADM(IE) Crisis 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	ADM(IE) Crisis Response Team - Annex A Incident and Consequence Guide – Annex B

Location Affected	Situation	Focus on:	Risk Management Strategies	Relevant DND Response Plans
	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	ADM(IE) Crisis Response Team - Annex A IT Disaster Recovery Team

Table 5 – ADM (IE) Situations and Response Plans

PART 3 – BCP MAINTENANCE, TRAINING AND EXERCISES

Plan Maintenance

31. 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.

BUSINESS CONTINUITY PLAN AMENDMENT HISTORY			
Change #	Date	Brief Description and Page Reference	Authorized By

Table 6 – BCP Amendment history

BCP Training and Exercises

32. Under development.

DRAFT V1.3

Annex A

ADM(IE)

BCP Implementation

ADM(IE) Crisis Response Team		
Name	Position	Responsibilities
Scott Stevenson	Level 1 Group Principal	• assessment of emergency and decision for on level of response required • authority to initiate any required spending •
Col R. Testa R. Davy G. Stones Cdr Dewar R.D. Edgecombe K. Brown J. Carter A. Bastarache	DGME DGRPP DGE A/DGNS DIECS/COS DIEIM DIEG Compt CEO CFHA	• assessment of emergency and decision on level of response required for ADM(IE) • authority to initiate any required spending •
R.D. Edgecombe	BCP L1 Coordinator	• co-ordination of corporate services activities •

Table A-1 – ADM (IE) Crisis Response Team

Resource Requirements	
Item	Description/Numbers
Workspaces/Offices	3 Offices to accommodate people and setup of IE Crisis Response Office to include computer, printer, telephone, fax machine)
Computers (desktops/laptops)	3 and connected to ADM(IE) Server
BlackBerry devices	Existing
Telephone & voicemail	Min 3 to support IE Crisis Office
Cellular Phone Digital	Existing (not new ones)
Secure Fax	Access to
Unclas Fax	Access to
< Note: This information is derived from the requirements outlined in ADM(IE) BIA >	

Table A-2 – ADM (IE) Resource Requirements

Mission Critical Systems, Applications and Databases		
Item	Responsibility / Contact	Recovery Time Objective
FMAS	IE Compt 4-2, J. Guest	Within 7 days
HAMIS Financial	CFHA Info Mgt, L. Gauthier	Within 30 days
HAMIS Housing	CFHA Info Mgt, L. Gauthier	Within 30 days
SMS Salary management system	CFHA Info Mgt, L. Gauthier	Within 30 days
CFEMS, CF Engineering Management System	DRAP 3-5-2, D. De Krom	Within 30 days
CMMS, Centralized Maintenance Mngt System	DRAP 3-5-2, D. De Krom	Within 30 days
CESS, Construction Engineering Supply System	DRAP 3-5-2, D. De Krom	Within 30 days
Pyramid, Project Management tool	Contractor S. Tagieff	Within 30 days
R3A, Real Asset Accrual Accounting	IE Compt 3-4, M. Bergeron	Within 30 days
RAIS, Realty Asset Information System	DRAP 3-2-2, C. Woermke	Within 30 days
EcoNet, Contaminated site/landfills	D Env P 3-2, J. Downey	Within 30 days
EcoNet, Fuel storage tank	D Env P 3-4, K.A. Fay	Within 30 days
HMS, Halocarbon Management System	D Env P 2-4, S. McFarlane and A/D ENV P 2, J. Park	Within 14 days
SpillNet, Spill reporting tool	D Env P 2-4, S. McFarlane	Within 14 days
PESTRec, Pesticide Records Keeping System	D Env S 4-4 R. Crétien	Within 30 days
NSICS, Nuclear Safety Information Control Sys	DNSC 3, CPO2 D. Carroll	Within 30 days
IFSMR, Integrated Fire Services Management Reporting system	CFMM3-3 L. Pagé	Within 2 days
AQMS, Air Quality Monitoring System	CFFM3-3 L. Pagé	Within 30 days
CFFM Audit Compliance Application	CFFM 4, A. Dallaire	Within 30 days
I&E GIS Portal	DRAP 3-3, G. Hamilton	Within 30 days
BASS, Business Application Support System	ADM(IE)/COS, RD. Edgecombe	Within 30 days
SIMS, Spatial Information Management System	DRAP 3-3, G. Hamilton	Within 30 days
WATERNET	DCPEP 9-5 J-C. Côté	Within 30 days

Table A-3 – Mission Critical System Applications & Databases

Vital Records		
Item	Location	Contact
SOPs for DGNS Technical Assistance Team (TAT)	Std Life Bldg	DNSA 3 Roger Hugron 995-9506
BCP Plan	ADM(IE)/COS Office	R.D Edgecombe 995-7243
Employee contact lists	L2 Offices	Ea ADM(IE) L2

Table A-4 – ADM (IE) Vital Records

Alternate Sites	
Primary	Pearkes Building (101 Colonel By Drive) 9NT ADM(IE) Ex Office Area
Secondary	Standard Life Building (275 Slater Street), DGNS Office Area
Alternate	Thurnston (2171 Thurnston), CFHA Office Area

Table A-5 – ADM (IE) Alternate Sites

DRAFT V1.3

Annex B

ADM(IE)

BCP Contact Information

BCP Response Team Contact List

BCP Response Team Contact List

Organization	Name	Address	Phone(W)	Phone(H)
Organization	Name	Address	Phone(W)	Phone(H)
ADMIE COS/DIECS	Edgecombe, Don	697 Apollo Way, Orleans, On	995-7243	613-830-8545
DIECS	Maj. Nadeau, Yves	1551 Delia Cr, Orleans, On	995-1694	613-841-2008
D Env P 4	Saydeh, Emmanuel	1395, Shalom St. Cumberland, On	995-4200	613-833-9051
COS DGME	LCol Ouellet, Luc	337 Rue Brébeuf, Gatineau Qc	995-6528	819-643-5850
DIEG Compt 4	Cdr Hatt, Murray	614 North Hampton Dr, Ottawa On	995-5362	613-824-7756
DIEIM Sr Proj Offr	LCol Perras, Claude	63 Rue Paquette,Gatineau, Qc	944-6181	819-663-4466
DGNS Plans & Ops	Princiotta, Melissa	1034 Tomkins Farm Cr, Ottawa, On	992-2498	613-822-2551
DRFM 3-3	Braun, Tracy	2744 Mozart Court, Ottawa, On	995-9470	613-260-9087
CFHA Gen Mgr	Porter, Robert	1911 Venus Avenue, Orleans, On	990-1406	613-824-4617

Table B-1 – ADM (IE) BCP Response Team Contact List

Employee Contact List

Employee Contact List

Organization	Name	Address	Phone(W)	Phone(H)
CFHA CEO	Bastarache, Alain	258 Mont Fleuri, Gatineau, Qc	998-5904	819-643-3808
D Env P	Berthiaume, Holmer	22 Birikett St. Nepean, On	995-8850	613-825-9250
DIEIM	Brown, Kathryn	610 Westview Ave. Ottawa, On	995-1064	613-761-9816
CFHA GM Compt	Carleton, Jill	3319 Drew Henry Dr. Osgoode, On	998-4941	613-818-2857
DIEG Compt	Carter, James	23 Carhidel Court, Ottawa On	995-7243	613-823-2705
DGRPP	Davy, Gerald	1539 Lakeshore Drive, Greely On	995-5586	613-821-2297
DRAP	Desjardins, Marc	1456 Laurin, Orleans, On	995-1162	613-834-3669
A/DGNS	Cdr Dewar, Keith	6433 Nathan Court, Ottawa, On	992-8546	613-830-8804
ADMIE COS/DIECS	Edgecombe, Don	697 Apollo Way, Orleans, On	995-7243	613-830-8545
DNSC - Dir	Cdr Dewar, Keith	6433 Nathan Court, Ottawa, On	992-8546	613-830-8804
ADMIE EA	Gibson, Jamie	2600 Draper Ave, Ottawa, On	945-7546	613-721-6204
DEEM	Godbout, Daniel	1380 Mountainside Cr. Orleans On	995-4072	613-837-8465
D Env S	Vacant			
CFHA A/GM PCC	MacKey, Lloyd	6859 South Village Dr, Greely, On	990-8223	613-821-1448
CFFM- Dir	LCol Morinville, Gaetan	60 Marie-Buyart, Gatineau, Qc	995-1959	819-243-8815
CFHA GM ITS	Nguyen, Van-Khanh	33 Rotchwell Dr, Gloucester On	996-4679	613-868-8878
CFHA GM CS	Louis Gauthier	281 Kinglet Way, Ottawa, On	998-1289	613-868-8105
DCAE	Paquet, Daniel	874 Paradise Cr, Orleans, On	995-1984	613-834-9504
DNSA-Dir	Pierre, Martin	340 Charles St South, Gananoque,On	996-0699	613-821-6130
Employee Contact List				
Organization	Name	Address	Phone(W)	Phone(H)

CFHA HO	Porter, Robert	1911 Venus Avenue, Orleans, On	990-1406	613-824-4617
DNR-Dir	Sigouin, Luc	2421 Brickland Dr. Cumberland, On	996-7722	613-833-2243
ADMIE	Stevenson, Sott	6 Brandy Creek Cres., Kanata, On	945-7544	613-271-1909
DGE	Stones, Ginger	359 Berkley Ave. Ottawa, On	995-0923	613-722-0487
DGME	Col Testa, Robert	Pending Posting in		

Table B-2 – ADM (IE) Employee Contact List

Note: Detailed employee contact list are maintained by individual ADM(IE) L2 organizations

DRAFT V1.3

Annex C

ADM(IE)

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

DRAFT V1.3

Annex D

ADM(IE)

BCP Planning Assumptions

Planning Assumptions

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 ADM(IE) preparedness and response structure:

Under development

DRAFT V1.3

Annex E

ADM(IE)

Key References

Key References

Government Security Policy (GSP):
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/gsp-psg_e.asp

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 100x-0 – Business Continuity Planning:
TBD

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

Comd-NET Home Page/Corporate/Business Continuity Planning

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

Organization and Accountability:
http://www.forces.gc.ca/site/minister/eng/authority/oa_e.htm

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

DND/CF Critical Infrastructure Protection Program:
TBD

DND/CF IT/IM Continuity Plan:
TBD

Management of Information Technology Security Standard (MITSS)
[GoC requirements for IT continuity planning are outlined in sections 12.8 & 18]:
http://publiservice.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/23RECON_e.asp

Management of Government Information Policy
[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/pubs_pol/gospubs/TBM_12A/CHAPT2-4_e.asp

DND/CF Security Plans and Instructions *[physical security]*:
http://vcds.mil.ca/cfpm/org/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

CF Exercise Program:
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/corporate/list_e.asp?value=all&lang=E&loid=326

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/

ADM(IE) SOPs… **Under development**