National Defence / Défense nationale

Level 2 BIA / BCP Workshop

Canada

Agenda

1. Introductions
2. Session Objectives
3. BIA/BCP Overview
4. Priority Discussion
5. Wrap-up and Questions

Objectives

By the end of this session, participants will:

a. Identify Priorities

b. Describe and rationalize each of the Priorities using:
   - timeframes
   - impacts
   - special situations
   - minimum service & resources required
   - alternatives
   - dependencies

c. Capture information and identify any follow-ups necessary to complete the BIA document

After the session:

a. Perform any follow-ups (other sessions, interviews)

b. Complete the BIA and use this information as a foundation for the L2 and L3's BCP Program strategy and direction.

DND/CF BCP Methodology

Establish clear lines of authority, accountability and responsibility

Affirm the role/mandate of the Department

- Protect Canadians at Home
- Defend North America
- Defend Canadian Interests Abroad

Step 1: Establish Departmental BCP Governance

Step 2: Affirm Departmental Role/Mandate

Identify the major threats/risks to the Department

Step 3: Conduct a Threat-Risk Assessment

- Loss of Staff (e.g. Pandemic Influenza)
- Loss/Disruption of Services (e.g. utilities)
- Loss/Disruption of Facilities (e.g. physical damage)

Business Continuity Planning: Development and timely execution of plans, measures, procedures and arrangements to ensure minimal or no interruption to critical operations and the continued availability of critical services and associated assets.

Step 4: Complete a Business Impact Analysis

Identify critical operations, functions, services and assets

Identify Maximum Allowable Downtimes (MAD) and Minimum Service Levels (MSLs)

Identify interdependencies/resources

Step 5: Prepare Continuity and Recovery Plans

Identify what plans and arrangements already exist

Develop continuity and recovery strategies

Step 6: Test/Validate Contingency Plans

Develop a training and exercise program

Step 7: Plan refinement/ maintenance

Incorporate lessons learned

Phase 1	Phase 2	Phase 3	Phase 4

Government Security Policy...

*to support the national interest and the Government of Canada's business objectives by **safeguarding employees and assets** and **assuring the continued delivery of services***

1. comply with prescribed fire safety and emergency measures
2. business continuity planning program to provide for the continued availability of critical services and assets
3. coordinate plans and procedures to move to heightened security levels in case of emergency and increased threat situations

Business Continuity Planning is ...

an all encompassing term which includes the development and timely execution of plans, measures, procedures and arrangements to ensure minimal or no disruption to the availability of critical services and assets

Government of Canada Security Policy

Understanding the Organization

Threat Assessment- What are the threats to our critical activities?

What are our critical activities? → **What so we use to deliver critical activities?** → **What is the Maximum Tolerable Period of Downtime?**

Prioritize activities according to their criticality to your group.

Allow Senior Management to define the boundaries of the BCP, according to which activities are to be recovered and which are not immediately considered.

Consider

People

Premises

Technology

Information

Supplies

Stakeholders

Also consider bare minimums needed for recovery of service.

How long could each in-scope activity be non-operational before it begins to impact your organization's achievement of business objectives.

This may vary according to time of month/year.

Recovery Time Objective

Defines specifically what needs to be provisioned for in the Business Continuity Strategy

Understanding the Organization

Impact Analysis (IA)

- Allows an organization to determine and document the impact of a disruption to its activities.

Identification of Critical Activities

- Enables an organization to define boundaries to it's business continuity plan by defining those activities most critical to meeting its operational objectives. Non-critical activities may still be important, but could be recovered after activities and without such immediate and rigorous planning.

Understanding the Organization

cont'

Determining Continuity Requirements-

Understanding what each of the critical activities will need to support recovery. Should include:

People – Core skill, knowledge and resources needed to operate the activity
Premises – Desks, workstations or similar needed to operate the activity
Technology – Application systems, connectivity, hardware and software needed
Information – Information needed to support operation or compliance requirements
Supplies – Critical supplies needed to recover
Stakeholders – Includes suppliers and customers needed to operate the activity

Evaluating threats to critical activities –

Performing a risk assessment to quantify threats to the availability and continuity of an organization

Determining Strategies

< Area >	< Strategy Options Include >
People	• Documentation (to allow other people to perform critical tasks) • Cross Training • Succession Planning • Use of Third Parties
Premises	• Alternate premises within an organization • Reciprocal agreements or service level agreements • Working from home
Technology	• Geographical resilience and failover • Warm or cold recovery
Information	• Technical solutions • Battle box solutions
Supplies	• Battle box solutions • Diversion of just in time supplies to another location • Agreements with third parties to obtain necessary stock at short notice
Stakeholders	• Vendor due diligence • Contractual requirements

Developing and Implementing a BCP Response

TIMELINE

Incident Response

- Confirm everyone's OK
- Confirm the nature of the incident & what it means for the organization
- Take control of the situation
- Contain the incident & invoke BCP (if needed)
- Communicate with stakeholders

Business Continuity

- Recover critical processes
- Maintain control of the situation
- Communicate with stakeholders
- Make sure everyone stays OK

Back to Normal

Focus

1. Consider the situation where one or more of the following ‘assets’ are unavailable in a ‘normal’ or ‘usual’ manner

    a. building(s)
    b. vehicles, tools, supplies, materials
    c. information / data
    d. application / systems
    e. communications
    f. people

2. The cause is not the focus

Typical Response

Severity	Impact	Typical Response
Minor disruption	Localized event affecting part of building with operations in other areas returned to normal in hours/day	Best Efforts
Disruption	Localized event affecting part of the building with operations in other areas returned to normal in a day/days	Focus on affected services, make space and resources available for time critical demands
Major Disruption	Local/Municipal events affecting the better part of the building with most operations returned to normal in a matter of days/week	Focus on critical services, EMRT to implement BCPs as required, relocate personnel, redirect telecommunications and re-establish systems
Catastrophe	Local/Municipal events affecting the building with all operations affected and where the facilities may not be inhabitable	Focus on critical services, ExCom to direct response and activation of contingency plans as required

Impact Analysis

1. Measures the impact of business functions not being operational

2. Provides business driven values that define the criticality of essential services and support services

3. Defines operational requirements for essential services, support services and dependencies (such as people, IT systems, work space equipment, and communications)

4. Arrangement can then be made to implement the selected strategies to facilitate recovery essential services, support services and dependencies

Impact Analysis

The business driven values that define the criticality of essential services and support services include:

A. **Maximum allowable downtime**

B. **Minimum required service levels and for how long**

C. **Recovery times for essential support services:**
   I. **Recovery time objectives for essential IT systems – based on the impact of IT systems being down**
   II. **Recovery times for other support services (HR, Finance, procurement, etc)**

Building the BIA Template

DND/CF
Continuity of Service/Operations Impact Analysis
Data Capture Worksheets

Tombstone Data

Functional Area:
Business Unit:
Responsible Manager/Director:
Location:
Mission/Mandate:

Continuity of Services/Operations Impact Analysis
Service/Activity Analysis Worksheet

What do you do?							
Inputs		Processes			Outputs[1]	Outcomes	Clients
Number of Staff	Incremental Costs	Description of Critical Activities /Services	Hrs of Operations	Surge Situations (Always /conditional /contingent)[2]			

[1] Reports, regulations, inspections certificates, etc.

[2] Is there a time of year or specific situation or event where the organization's resources are involved in dealing with the issue to the exclusion of normal daily operations (no – what we do is always critical, sometimes – when this situation occurs we are conditioned to respond direct our attention to resolving it, maybe, who knows – there are things that could happen and in those situations we have contingent processes and procedures to deal with it).

Continuity of Services/Operations Impact Analysis
Critical Services Analysis Worksheet

What is critical about it?					
Priority	**Critical Activities/process**	**Rationale – Mission / mandate of organization in relation to the national or departmental interests[1]**	**Quantitative Costs / Losses[2]**	**Qualitative Costs / Losses[3]**	**Risk Statement (impact level)**

National Interest - Health, safety, security, economic well-being, effective functioning of government, credibility and public confidence.

Departmental Interest - legal/contractual, regulatory, time sensitivity.

Quantitative: impacts are usually expressed in terms of avoidable financial costs and the costs of injury to clients and Canadians in general if services are not delivered within normal time periods. These include the cost of injury that would occur if services were not delivered: legal liability (fines), backlog costs, economic losses (fees)

Qualitative: impacts are intangible losses that can affect the credibility or reputation of the department or the GOC for example: loss of clients trust, violation of security policy or legislative requirements, etc.

High – high injury will generally result in such things as loss of life, the breakdown of civil order (e.g. violent demonstrations), loss of territorial sovereignty, irreparable loss of public confidence, extremely large financial losses or severe disruption to the economy, disclosure of intelligence sources or methods of gathering intelligence, serious long-term damage to the conduct of international relations, and unavailability of a critical service. Medium – medium injury will generally result in such things as injury or illness to individuals, inability to conduct criminal investigations or other impediments to effective law enforcement, serious loss of public confidence, compromise of particularly sensitive personal information, significant financial loss or disruption to the economy, ineffectiveness in conducting international or federal-provincial relations, and disruption of services that would seriously inconvenience Canadians. Low – low injury will generally result in such things as public embarrassment, minor financial loss, and inconvenience in conducting fed-prov or international relations and minor disruption of internal government operations leading to delays & loss of information.

Continuity of Services/Operations Impact Analysis
Downtime, Staff Requirements and Minimum Service Levels Worksheet

When do we need to be back on-line?							When do you need staff and in what amounts?					
Critical Activities / Processes[1]	Maximum Allowable Downtime						Human resource requirements over time					
	Hours		Days		Weeks		Hours		Days		Weeks	
	0-4 hrs	<24 hrs	24-48 hrs	2-5 days	6-10 days	10-30 days	0-4 hrs	<24 hrs	24-48 hrs	2-5 days	6-10 days	10-30 days

[1] The minimum acceptable level of the service – the point at which a high degree of injury would result.

[1] Services deemed in the National or Departmental Interest AND where there is a Level 1 risk if the service is not delivered (from Critical Services Analysis Worksheet).

Continuity of Services/Operations Impact Analysis
Downtime, Staff Requirements and Minimum Service Levels Worksheet

(con't)

What is the minimum level of services you need to provide?	Comments/ Justification
Minimum Service Levels[1]	

[1] The minimum acceptable level of the service – the point at which a high degree of injury would result.

Continuity of Services/Operations Impact Analysis
Dependencies Analysis Worksheet

Who or What do you depend on to deliver your service?							
Critical Activities / Processes[1]	**Suppliers**	**Other Government Departments**	**Other DND Branches Directorates**	**Other Corporate Services**	**Infrastructure (facilities, telecom)**	**Databases/Vital Records**	**IT Systems / Applications**

[1] Services deemed in the National or Departmental Interest AND where there is a Level 1 risk if the service is not delivered (from Critical Services Analysis Worksheet)

Continuity of Service/Operations Impact Analysis Recovery Strategies and Resource Requirements Analysis Worksheet

What do you need to do to ensure the delivery of critical services?						What resources do you need to provide a minimum service level of critical services?		
	Alternate Strategies[9]					Resource Requirements[10]		
Critical Activities / Processes	Succession plans/ cross trained staff/ detailed SOPs	Alternate sites[11] (staff relocation)	Re-establish systems and network interfaces	Establish Comms	Alternate means (Telework/ virtual officing/ other service providers)			

9 Identifying whether the strategy is in place or required
10 Data elements to be identified by relevant responsibility centre
11 Identify your alternate site if known

Business Continuity Plan Contents

Task and Actions Lists

A. The BCP should include task lists and action plans. These tend to be more prescriptive than incident management task or action lists, and are designed to support a known invocation process.

Roles and Responsibilities

A. Clarifying management roles and responsibilities win a BCP situation when the operational management is unavailable

Business Continuity Plan Contents

Recovery Locations

A. Details, including directions to, recovery locations or alternate processing facilities

Stakeholder Management

A. Details of key stakeholders, their contact locations and how they are to be communicated with

Business Continuity Plan Contents

Battle Box Location

A. If a battle box has been created, where it is stored and how it is recovered.

IT Disaster Recovery

A. How systems are recovered, including equipment sourcing, backup recovery and restoration, order of recovery and changing telecommunications links. This sometimes forms an additional plan itself.

General BCP Assumptions

- the disruption/dislocation is only temporary
- only your building or processes are affected by a disruption
- at least one form of communications is available
- qualified personnel in sufficient numbers are available
- back-ups are done as directed, alternate arrangements made

General BCP Assumptions

- critical back-up files and information held off-site are intact
- external stakeholders will be reasonably cooperative
- plans are reviewed, maintained and tested regularly
- training is done and people are aware
- for every position identified there are incumbents and alternates

Anatomy of a BCP

- who is responsible for decision making (BCP Response Team) and for implementation of response measures (key personnel)?
- what are they responsible for (what critical services/functions and what is the minimum acceptable level of services) and what are we dependent on (infrastructure, support)?
- where will these services be provided from (alternate site)?
- who do we have to contact to let them know the situation (contact lists – employees, clients, corporate services, vendors)?
- how do we go about recovering services (what steps need to be taken to implement/provide service)?

Sample Appendix for Level 2 and 3
Level 2and 3 Continuity Requirements and Fan-out List Templates

Group: **Branch:**		**Director General:** **Director:** **Manager:**
Location:		
Critical Services (in order of Priority) **1:** **2:** **3:**		
" *BCP Support Team Members* "		
Name/Position	**Role**	**Responsibilities**
		• ***Oversee Response***
		• **Etc.**
		• **Etc.**
		• **Etc.**

Sample Appendix for Level 2 and 3
Level 2 and 3 Continuity Requirements and Fan-out List Templates (con't)

Resource Requirements:	
❑ 1 phone set with voice mail ❑ Closed office ❑ Access to DWAN ❑ Access to Databases (specify which data bases)_____ ❑ Secure fax ❑ Titan	❑ Remote Access with high-speed Internet connectivity ❑ Etc.
Relevant Documents:	
❑ BCP Documents ❑ Incident and Consequence Management Guide ❑ Building Emergency Evacuation Plans ❑ Relevant SOPs	❑ Contingency plans ❑ Etc.
Alternate Sites:	
Primary	
Secondary	
Tertiary	

Contact List

Identify all those individuals that have been deemed critical and provide the required information below:

Contact List:					
L2 Group XXXX					
Name:	**Address:**	**Work:**	**Home:**	**Cell:**	**Email:**

Your contact list identifies all those people that are required should your BCP be invoked. Your fan-out list would be used to inform all personnel of the current situation.

Appendices ...

1. Levels of Service
2. Contact Lists (Response Team, Employees, Offices, Corporate, Suppliers, Clients)
3. Critical Assets (systems, equipment, databases)
4. Forms and Locators

Sherryl.booth@rogers.com
William.hitchins@forces.gc.ca