OVERVIEW OF

BUSINESS CONTINUITY PLANNING

Presentation to the BCP Working Group

21 Feb 07

C.J. Cowan, DGCSS Senior Analyst
DND BCP Co-Coordinator

Outline

- Policy requiring BCP
- Overview of BCP
- BCP Elements
- What matters most
- Questions

Continuity of Government

- The Department of Public Safety and Emergency Preparedness (PSEPC) has established a Continuity of Government Program to ensure in excess of 150 federal departments are able to:

1. Protect the safety and health of employees in disruptions;
2. manage the risks of disruptions;
3. deal with critical infrastructure failures and slow-downs;
4. deliver critical services at acceptable levels in a disruption; and,
5. minimize the impacts of disruptions on operations.

Taken from PSEPC BCP Presentation

TBS 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***

- TBS Requires Departments to:
  - comply with prescribed fire safety and emergency measures
  - develop a **business continuity planning program** to provide for the continued availability of critical services and assets
  - coordinate plans and procedures to move to heightened security levels in case of emergency and increased threat situations

BCP Program Requirement/Definitions

- **In accordance with the Government Security Policy (GSP), TBS has mandated that all departments establish a Business Continuity Planning (BCP) Program to provide for the continued availability of:**

  "Services and associated assets that are critical to the health, safety, security or economic well being of Canadians, or to the efficient functioning of the Government of Canada."

- **Critical services are DND/CF services whose compromise in terms of availability or integrity would result in a high degree of injury to the health, safety, security or economic well being of Canadians, or to the efficient functioning of the Government of Canada. BCP Program assures Minimum Service Levels (MSL) for critical services.**

- **High degree of injury is severe harm related to the provision of sustenance (e.g food, water, shelter, energy), public order, emergency care and response, a life sustaining environment, vital communications and transportation, fundamental economic services, continuity of government, territorial integrity and sovereignty.**

What is BCP?

- **The federal Government Security Policy defines BCP as:**

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

- **"All-encompassing"** means that BCP provides a framework for many types of planning, including emergency response planning, IT/IM continuity planning, crisis management and risk planning

Business Continuity Planning is:

- the process of ensuring ongoing business operations in the face of disruptive events

- principally a management plan whose scope includes the Disaster Recovery Plan and other plans such as emergency response and crisis management plans.

Terminology Soup

Business Continuity Plan

Disaster Recovery Plan

End-user Recovery Plan

Contingency Plan

Emergency Response Plan

Crisis Management Plan

Emergency Preparedness Plan

Taken from DNIS Presentation on Disaster Recovery

Key Plans

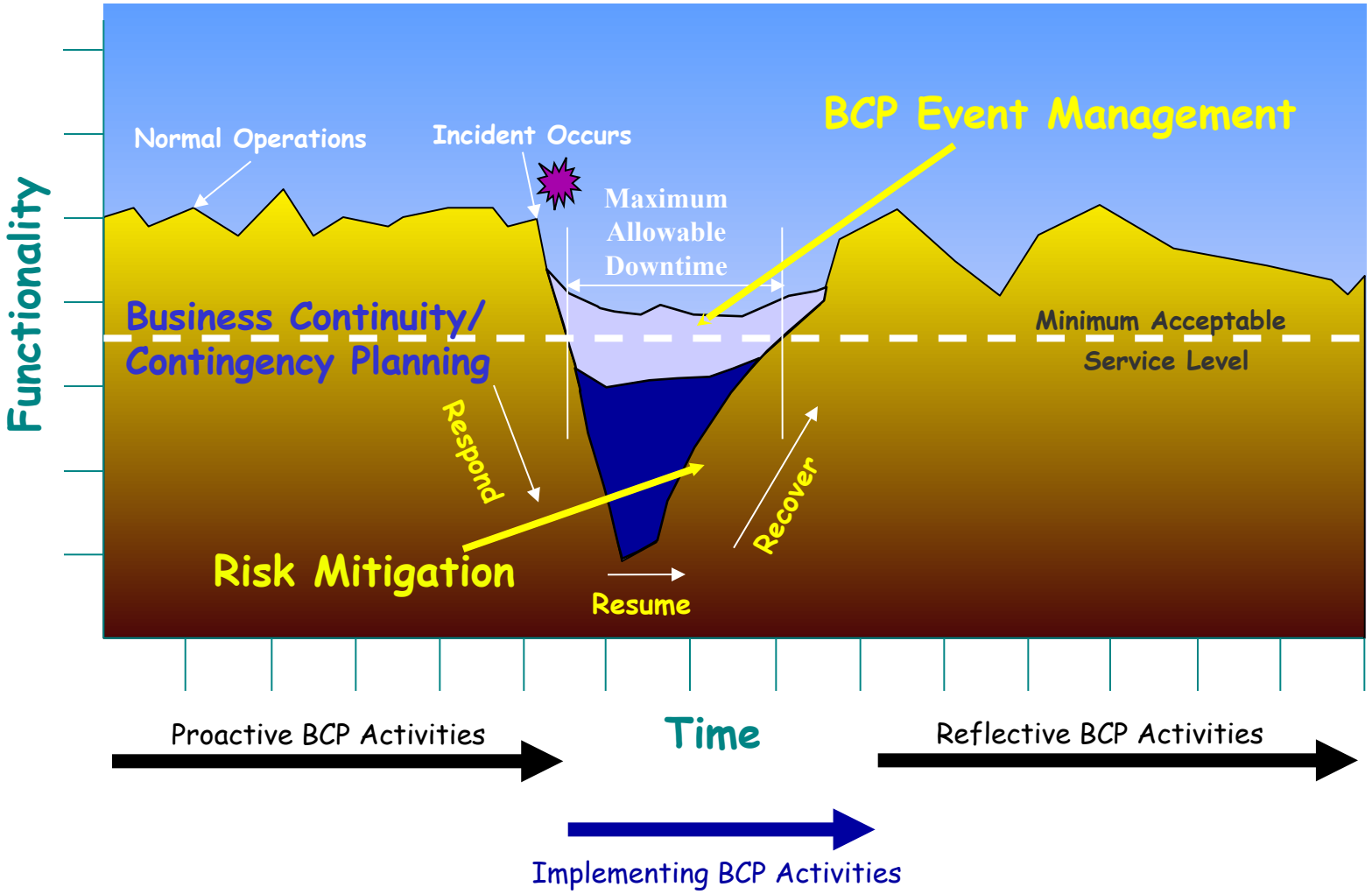
- **Contingency Plan/Emergency Response Plan (ERP)**
  - A contingency plan, also called an emergency response plan, is a set of procedures to be followed in order to minimize the effects of an abnormal event. It serves as a guide or reminder of the steps to take during an emergency response and identifies personnel and their responsibilities.
- **Emergency Preparedness Plan (EPP)**
  - Describes activities, programs, and systems used for response, recovery, and mitigation in anticipated emergencies
  - Details how the organization plans to ensure that it is equipped, trained and prepared to execute the emergency response/ contingency plans in response to domestic emergency situations
- **Disaster Recovery Plan**
  - Deals with recovering assets after a disastrous interruption or damage

Business Continuity Plan

- provides the framework for a common management structure under which all emergencies and disruptive events can be managed
- Enables critical services or functions to be continually delivered.
- Complements emergency preparedness (e.g. fire and building evacuation, civil emergency plans)
- also supports planning that is necessary to restore other-than-critical services and their associated assets and resources

- **Instead of focusing on reactive measures (i.e. emergency response, resuming a business after critical operations have ceased or recovering after a disaster), a Business Continuity Plan is a proactive plan that endeavours to ensure that critical operations continue to be available**

Event Horizon



Adapted from: DoD Office of Contingency Planning

Recent Situations

Water/Air/Env/Fire damage or contamination

Occupational Safety & Health concerns, Work place relocation of critical services

e.g. Anthrax scares, Water contamination L'Esplanade Laurier

Public Sector Strike

Workplace accessible however there was potential to limit access to staff, broader impact

SARS

Public Health Emergency, Health of Ontarians/Canadians

9/11

Attack on a nation

The Big Blackout 2003

Average Outage Time*

- Fire – 28 days
- Internal Power – 22 days
- Flood – 10 days
- IT Failure – 10 days
- External Power – 1 + days

[1] based on UK Stats as reported in Computer Weekly

Anatomy of a BCP

- Who is responsible for decision making 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)?

BCP Elements

- BCP Elements as per Government BCP Operational Standard
  - Governance
  - Business Impact Analysis
  - Plans and Arrangements
  - BCP Readiness

TRA Considerations

- Identify **resources** at risk (personnel, assets, information, facilities)
- Identify **threats** to those resources (Terrorists, hackers, disgruntled employees, natural disasters that could cause harm - disclosure, interruption, modification, destruction, removal of mission critical resources)
- Determine **vulnerability** to the threats (confidentiality, integrity, **availability**, authenticity, non-repudiation, isolation, authorization)
- Calculate **losses** from exploiting vulnerability
- Assess **safeguards** to transfer or mitigate losses

Source: RCMP Guide to Threat and Risk Assessments

Business Impact Analysis

... identify and prioritize the department's critical services and assets - health, safety, security or economic well being of Canadians; the efficient functioning (continuity) of government; and, other services and assets when warranted by a TRA

Process

- ***Identify Critical Services***
- ***Document Processes and Resource Requirements***
- ***Prioritize (Max Acceptable Downtime/Min Service Levels)***

Critical Services ...

a service whose compromise in terms of availability or integrity would result in a high degree of injury to the health, safety, security or economic well being of Canadians or the efficient functioning of government

Source: GoC GSP

business activities or information that cannot be interrupted or unavailable for several business days without significantly jeopardizing operation of the organization

Source: DRI International

Typically a BCP is the means by which departments "guarantee" service delivery

What Matters Most* ...

- Supporting the Governments response to national or regional emergencies
- **Fulfilling other statutory, regulatory and financial obligations**
- Maintaining operational service delivery capacity
- **Sustaining corporate support and maintaining critical infrastructures**
- Communicating with stakeholders

* - what matters most is situation dependant ie: nature, presentation, extent, severity, impact

Key References

- www.tbs-sct.gc.ca
  - Government Security Policy
  - Operational Security Standard – Business Continuity Planning (BCP Program)
  - Emergency Preparedness Act
  - Emergencies Act
  - Pandemic Planning Template
- DND:
  - DM/CDS Initiating Directive, 5 Jan 07
  - CF/DND Contingency Plan for the Response to a Pandemic Influenza, 30 Jan 07

Questions?