

DEFINITIONS

🌐 **Crisis** - a situation that challenges one's sense of appropriateness, tradition, values, safety, security or the integrity of government

🌐 **Emergency** - an abnormal situation that requires prompt action, beyond normal procedures to limit damage to persons, property or the environment

🌐 **Service Disruption** - a situation that results in an interruption in the provision of critical services (denied / limited access to people, systems / processes, workspaces)

🌐 **MAD**- Maximum allowable downtime

🌐 **MSL**- Minimum Service Level

🌐 **Recovery Time Objective (RTO)**- the point in time when you must have at least the critical aspects of your business operational again

"The initial response to the crisis sets the tone for the rest of the effort."

(Shrivastava - Bhopal, Anatomy of a Crisis 1987)

WHAT IS BUSINESS CONTINUITY PLANNING?

What's This??



(Courtesy KIRW)

Looking Serious



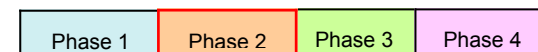
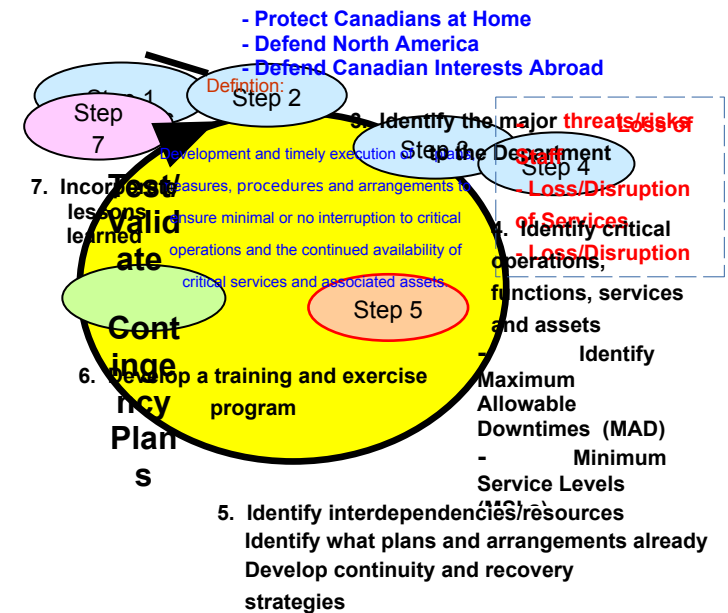
(Courtesy KIRW)

Very Serious!!!



DND/CF BCP Methodology

1. Establish clear lines of authority, accountability and responsibility
2. Affirm the **role/mandate** of the Department



Business Continuity Plans

Business Continuity Plans (BCPs) are developed to ensure minimal or no interruption to the availability of critical approaches to resume operations in the face of potential disruptions. Proactive measures are planned and implemented before the occurrence of a disruption to mitigate the consequences of such incident while reactive measures are activated upon a disruption being detected.

Purpose

- Provide predetermined actions to allow prompt resumptions of critical functions
- Reduce decision making during recovery operations
- Allow return to normal operating conditions at the earliest possible time
- Minimize financial loss and hardship
- Minimize extent of interruption

Enabling Business Continuity

The Six Steps to Success...

1. Understand what is important to your group

- What are the priority services that need to be

delivered following an incident (using a **Business Impact Analysis**)

- What processes deliver those services?
- How long can your group operate at a reduced level of service?
- What is the appetite for risk?

2. Achieve sponsorship and internal ownership

- Understand current capability
- Establish internal and external drivers (e.g. dependency upon IT, scope of insurance, extent of regulation and legislation)
- Develop training and awareness programmes

3. Develop a Business Continuity Plan

- What it needs, not **wants** to ensure continuity of business for your group
- Establish how to protect the activities of people, business processes/operations and IT infrastructure

- Establish the resources required to deliver priority services
- Create a crisis management structure to provide escalation, command and control, communication and co-ordination
- Align IT service and business process recovery

4. Implement, test and review

- Ensure joint testing, involving IT and business process recovery
- Progressive complexity with clear objectives
- Include crisis management exercises

5. Complement other risk management controls

- Risk reduction
- Risk transfer (insurance)
- Risk acceptance
- Risk avoidance

6. Build and maintain capability

- Crisis management (command and control)

- Recovery strategy (what your solution needs to look like)
- Plan documentation (codify the process, roles and responsibilities, contact details)
- Recovery process (outline how services will be recovered)
- External dependencies (understand supply chain dependencies and capabilities)
- Executive endorsement (budget, testing, training, accountability, audit and review)

Redundancy

Hot-Warm –Cold

“HOT” Service

Real time Recovery, automated -
No Fail (\$\$\$)

A hot site is a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data. Real time synchronization between the two sites may be used to completely mirror the data environment of the original site using wide area network links and specialized software.

“Warm Site” Service

Low-delay recovery, manual service **(\$\$)**

A warm site is a location where the organisation can relocate to after the disruption that is already stocked with computer hardware similar to that of the original site, but does not contain backed up copies of data and information. It may or may not have the same capacity as the original site depending on the organisation's requirements. Data will have to be restored onto the equipment at this site before activities can re-commence.

“Cold Site” Service

Longer delay recovery, high manual intervention **(\$)**

A cold site is the most inexpensive type of backup site for an organization to operate. It does not include backed up copies of data and information from the original location of the organization, nor does it include hardware already set up. The lack of hardware contributes to the minimal startup costs of the cold site, but requires additional time following the disaster to have the operation running at a capacity close to that prior to the disaster.

