



Business Continuity Management

... a Birdseye View



What's this???





Looking Serious



(Courtesy KRMV)



Very Serious!!!





Time For The BCP





Business Continuity Management ... a Birdseye View

- 1. The Big Picture**
- 2. What are we Dealing With**
- 3. Managing the Program**
- 4. Dealing with Service Disruptions**
- 5. Issues for BCP Practitioners**



The Big Picture

**... managing the
abnormal**



Managing the Abnormal

Not delivering critical services can and will escalate into a crisis if not handled



Mishandling of emergencies can and will escalate into a crisis

Inability to respond in an emergency compromises health, safety and security



Some 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)



Things that go Bump ...

**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

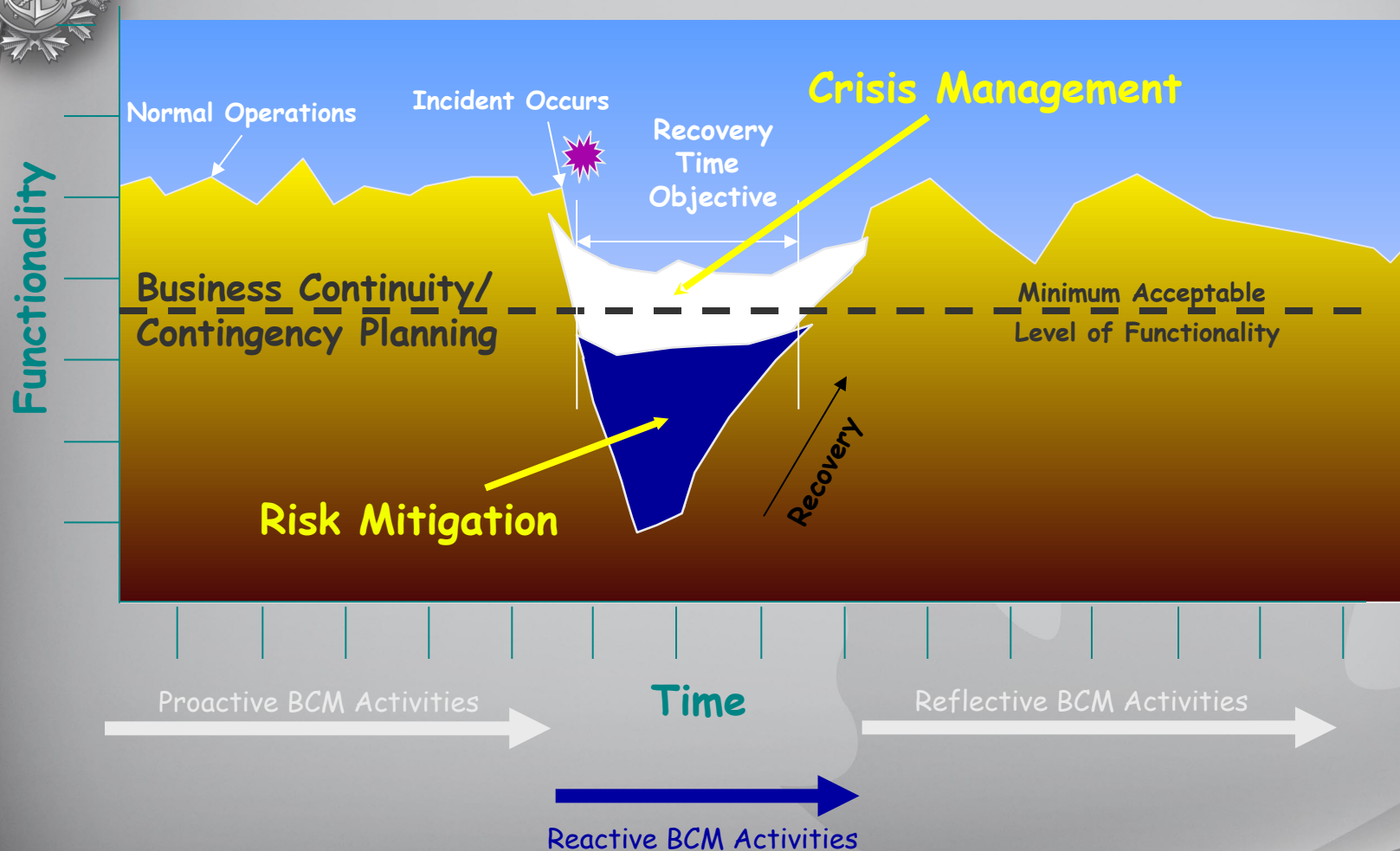
The Big Blackout

Affects the entire Eastern Region, TBS
mandates only critical services
operate

H1N1 Swine Flu



Event Horizon





What are we dealing with?

**... things that go bump
in the night**



What Do We Have to Worry About?

1. **Natural Disasters**
ice storm, earthquake, tornado, flood, hurricane
2. **Man-Made**
fire, explosion, water damage, bomb/CBRN, gas leak, Hazmat, civil disturbance, labour relations (strike)
3. **Technological**
power outage, telecommunications outage, infection, hackers, computer failure
4. **Biological**
contagions (SARS, Influenza, H1N1 Flu), infestation



How Bad Can It Get - Average Outage Time*

1. Fire – 28 days
2. Internal Power – 22 days
3. Flood – 10 days
4. IT Failure – 10 days
5. External Power – 1 day

¹based on UK Stats as reported in Computer Weekly



Where are we coming from?

**... policies, standards
and guidelines oh my**



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***

- comply with prescribed fire safety and emergency measures
- 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



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

*the process of developing advance **arrangements and procedures** that enable an organization to respond to an event in such a manner that **critical business functions** continue without **interruption or essential change***

Disaster Recovery Institute

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)

Step 5:
Prepare Continuity and
Recovery Plans

Identify interdependencies/resources

Identify what plans and arrangements already exist
Develop continuity and recovery strategies

Phase 1

Phase 2

Phase 3

Phase 4

Step 7:
Plan refinement/
maintenance

Incorporate
lessons learned

Step 6:
Test/Validate
Contingency Plans

Develop a training and exercise
program

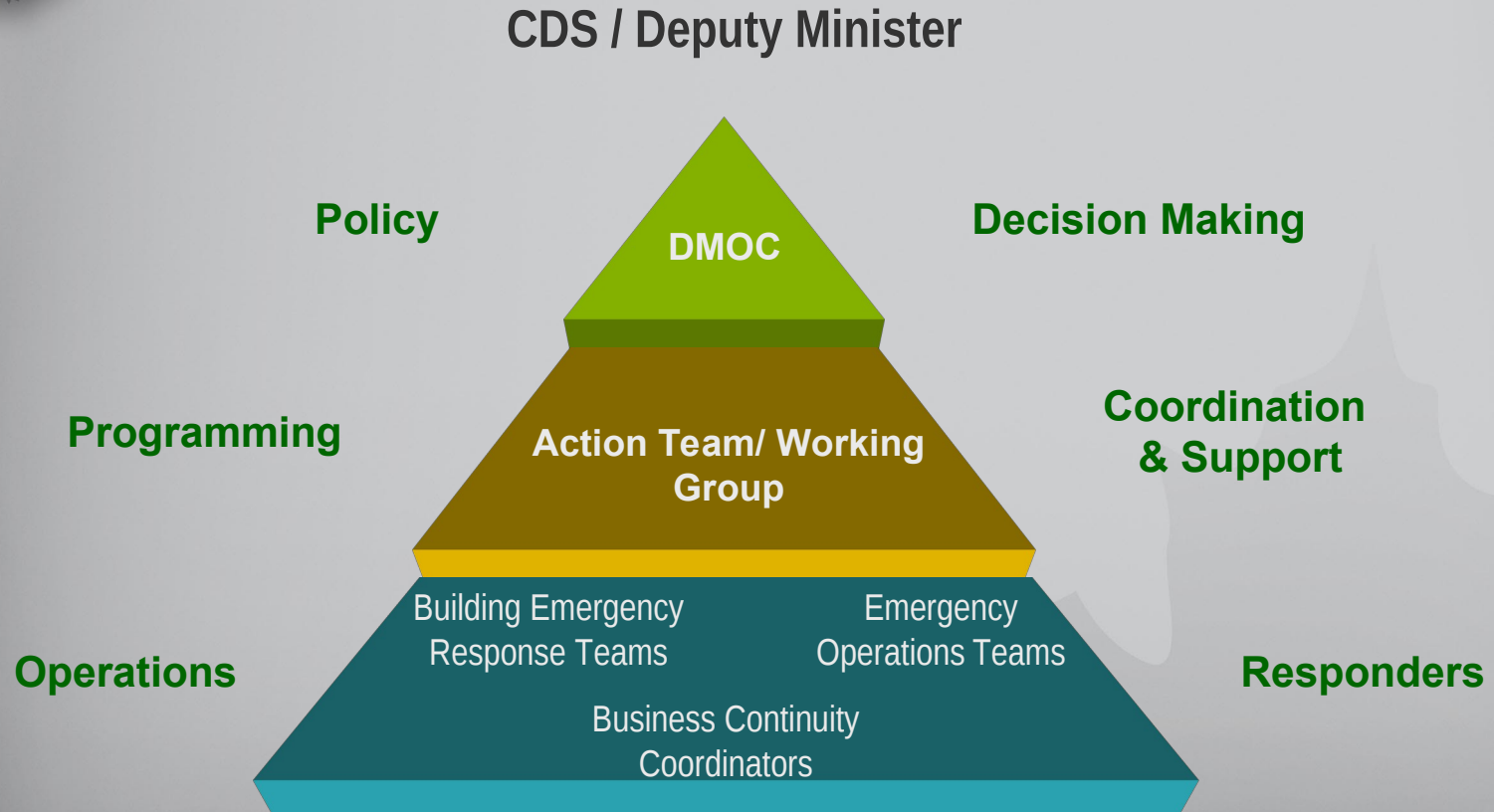


Governance

... Who does what?



Governance Structure - Best Practice



L0 Governance Structure



Roles and Responsibilities

	Preparedness	Response and Recovery
Executive Committee "policy direction"	<input type="checkbox"/> Strategic direction & policy approval <input type="checkbox"/> Review & approve critical services, BCPs <input type="checkbox"/> Establish maximum acceptable down-time & recovery objectives <input type="checkbox"/> Appoint Departmental Coordinator and oversee program <input type="checkbox"/> Allocation of resources	<input type="checkbox"/> Prioritizing response efforts <input type="checkbox"/> Plan and EOC activation <input type="checkbox"/> Approve recovery strategy <input type="checkbox"/> Communicates/coordination of OGDs <input type="checkbox"/> Approve extraordinary resources
BCP Working Group "policy development"	<input type="checkbox"/> Identify critical services & assess impacts <input type="checkbox"/> Identify threats and assess risks <input type="checkbox"/> Recommend risk management strategies <input type="checkbox"/> Approve plans <input type="checkbox"/> Oversee program implementation, monitor and provide assurances on preparedness <input type="checkbox"/> Provide training and awareness	<input type="checkbox"/> Assess extent of situation <input type="checkbox"/> Develop recovery strategy <input type="checkbox"/> Manage/coordinate/support response efforts <input type="checkbox"/> Monitor and report on status
Response Teams "policy implementation"	<input type="checkbox"/> Develop recovery measures <input type="checkbox"/> Draft plans <input type="checkbox"/> Make alternate arrangements <input type="checkbox"/> Review, test and update plans	<input type="checkbox"/> Secure site, assess and report on situation <input type="checkbox"/> Inform stakeholders <input type="checkbox"/> Implement plans as directed



Terms of Reference for an Emergency Management Steering Committee

1. Purpose – oversee program and advise on response
2. Scope
3. Authorities
4. Responsibilities of Steering Committee
 - Determining roles and responsibilities
 - Direction on Emergency Management Policy
 - Directing emergency management organization
 - Approving plans and activities
 - Ensuring training, reviews, testing, and audits are conducted
 - Advising on emergency response actions
 - Sourcing funding and committing resources
 - Resolving conflicts



Business Continuity Policy

- **Policy Statement – DND/CF has established a business continuity planning program to provide for the continued availability of critical services and assets, and will ensure that business continuity plans are developed, implemented and maintained. (DOAD 1003-0)**
- **Objective – to ensure that business continuity planning is managed throughout DND/CF to ensure the effective coordination and recovery of essential business functions and services in the event of an interruption.**



Business Continuity Policy (con' t)

- **Application – all L2 and L3**
- **Requirements – infrastructure, framework, roles & responsibilities**
- **Accountability – administration, audit**
- **Related Documents – Crisis Management Plan, Building Emergency, Departmental Emergency Plan, Continuity of Operations**



What Are We Really Trying to Do?

Identify the cost (*impact*) of a service disruption to set recovery objectives (*who's on first, when and to what extent*) and build a business case for implementing risk management strategies (*mitigation, planning & preparing for, responding to and recovering from*) for abnormal situations



Threats, Vulnerabilities and Risk

**... What could go
wrong?**



What is a TRA ?

A threat assessment is an evaluation of the nature, *likelihood* and *consequence* of acts or events that could place sensitive information and assets at risk.

A risk assessment is an evaluation, based on the effectiveness of current or proposed *safeguards*, of the chance of vulnerabilities being exploited.



How to do a TRA

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



Threat Mapping

Organizational Threats

- 1.Strategic** (political, economic, social, technological)
- 2.Business** (market, information, performance)
- 3.Operational** (lands, buildings, equipment, people, technology)
- 4.Financial** (revenue, cost, cash, investments, credit)

Crisis Types¹

- 1. Economic** (strikes, stock drops, market crash)
- 2. Human Resource** (loss of executives/personnel, work violence)
- 3. Informational** (confidentiality, integrity, privacy)
- 4. Physical** (facilities, infrastructure)
- 5. Natural Disasters** (quakes, ice storm)
- 6. Psychopathic Acts** (kidnapping, hostages, terrorism)
- 7. Reputation** (slander, rumor)

Services Hazards

- 1. Natural Disasters** (quakes, ice storms)
- 2. Man-Made** (fire, explosions, hazmat, civil disturbance)
- 3. Technological** (power outage, telecoms outage, computer failure)
- 4. Biological** (contagions – SARS, Avian Flu, West Nile, infestations – mold)



Who Do We Have to Worry About?

1. Internal

- A. Employees
- B. Contractors
- C. Couriers
- D. Maintenance Staff

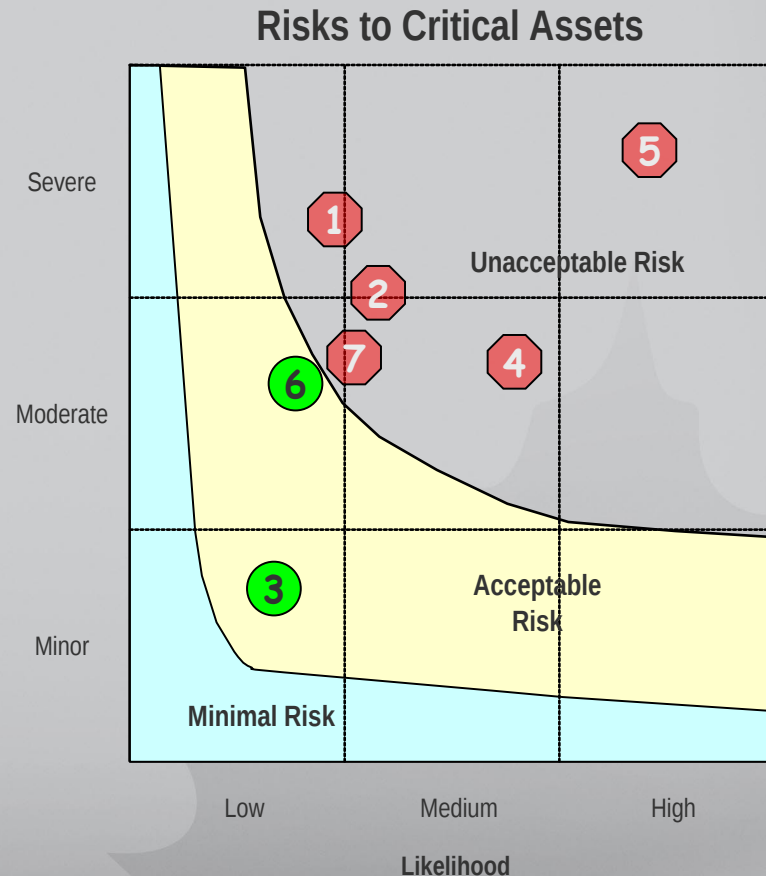
2. External

- A. Other Governments
- B. Criminals
- C. Terrorists
- D. Special Interest Groups
- E. Media
- F. Opportunists



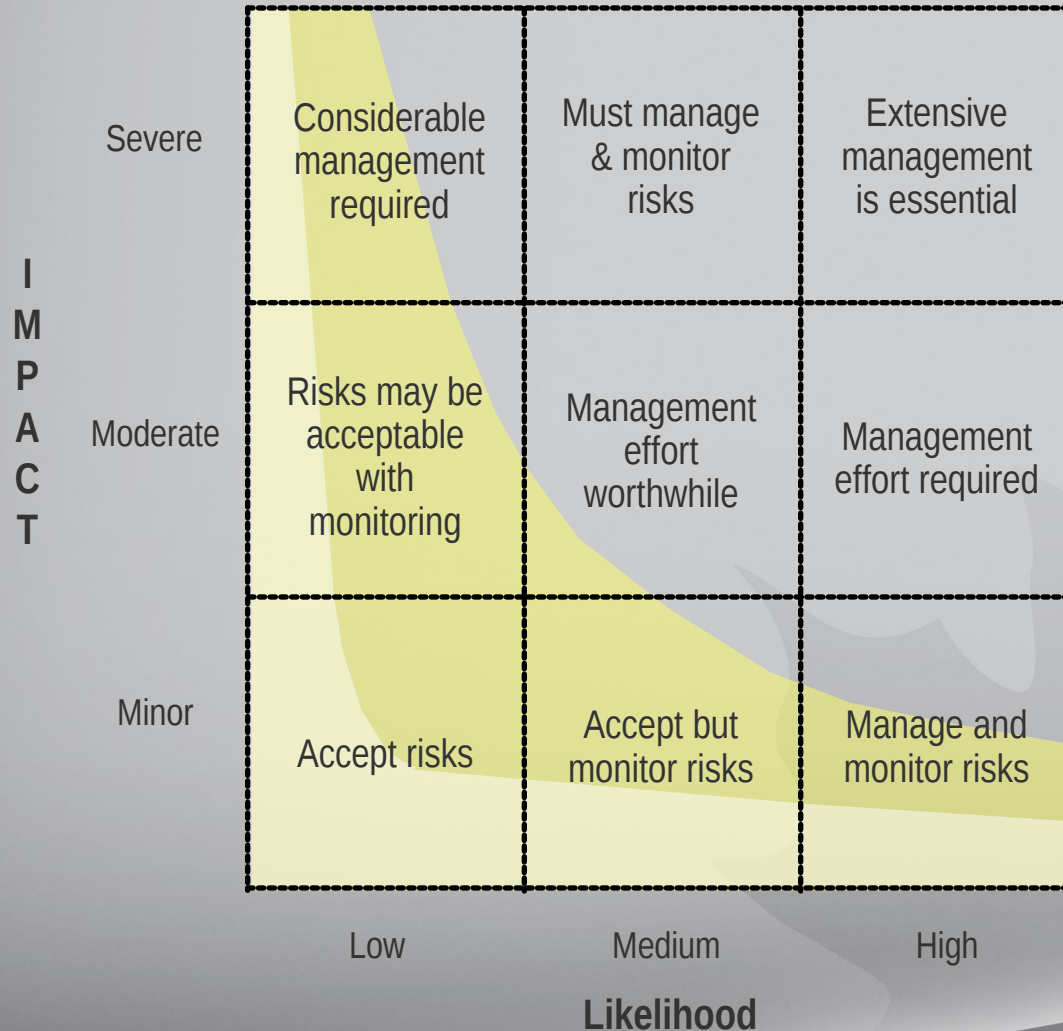
Risk Scorecard - Overall

- 1 • Personnel security
- 2 • Information Assets – Electronic
- 3 • Information Assets – Hard Copy
- 4 • Facilities
- 5 • IT Systems
- 6 • Attractive Assets (laptops)
- 7 • Services





Risk Management Model*





DND/CF Identified TRA results

The DND/CF TRA identified a wide variety of events that could affect operations and services.

- a) A loss of staff, e.g. due to 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.**



Recovery Strategies

1. Do Nothing / Defer / Best Efforts
2. Work Area Recovery and Manual Work Around
3. IT Disaster Recovery / Distributed Processing
4. Telecommunications Recovery
5. Alternate Site/Staff Relocation
6. Alternate Sourcing
7. Ship-in Services
8. Salvage Procedures
9. Shared Services



Risk Management Strategies

Mitigate

1. Backup Strategy
2. Alternate Site
3. Archive Strategy
4. Access Controls

Plan & Prepare

1. Disaster Recovery / IT Continuity Plans
2. Business Continuity Plans
3. Crisis Management Plan
4. Mapping Architecture
5. Training / Exercises

Respond & Recover

1. Best Efforts
2. Alternate Site
3. Crisis Management Guide
4. Arrangements
5. EOC/Command Centre



Business Impacts Analysis

**... Focusing on What
Matters**



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 of government; and, other services and assets when warranted by a TRA

Process

1. *Identify Critical Services*
2. *Document Processes and Resource Requirements*
3. *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



How to do a BIA

1. **Developing the BIA Project Plan**
2. **Pre-Planning and Creating the Survey**
3. **Launching the Project**
4. **Distributing the Survey and Collecting Information**
5. **Analyzing the Survey Results**
6. **Presenting Survey Findings to Senior Management**
7. **Gaining Senior Management Approval to go to the Next Step. (developing specific continuity plans)**

Source: BCP Training Course – Training and Development Canada



How to Figure Out What Matters

1. **BIA Questionnaire / Survey**
 - A. Thorough but time consuming, chasing people for input, interpreting results an art
2. **Interviews**
 - A. Less thorough but still time consuming, judgmental, isolated, objectivity concerns
3. **Computer based**
 - A. Do the underlying assumptions apply?
4. **Workshops**
 - A. Consensus builder, better discussion of risk and inter-dependencies
5. **Research / Evaluations**
 - A. Thorough and inclusive, look to see if scope/objectives apply



Sources ...

1. Legislation, regulations, contracts etc.
2. BIAs / TRAs etc.
3. Audit Reports
4. Internal Reports (financial, marketing, business case, performance)
5. Process Modeling / Maps
6. Loss / Incident reports
7. Schedules
8. Client Surveys



Impact Assessment

1. **Determine the nature of the business and services it must deliver according to:** legislation; government policy; or, obligations stemming from OGDs or other service arrangements, treaties, contracts, MOU/As
2. **Assess services to determine those that cause severe injuries from a disruption in service**
3. **Severe injuries are ones that cause immediate and direct harm related to:** provision of sustenance; public order; emergency care and response; a life sustaining environment; vital communications and transportation; fundamental economic services; **continuity of government**; and, territorial integrity and sovereignty



What Matters Most* ...

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

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



Recovery Objectives

Need to determine

- a) Maximum Allowable Downtime**
- b) Minimum Acceptable Service Levels**

Dependant on

- a) specific obligations (contract terms and conditions)**
- b) client expectations (service level commitments)**
- c) dependencies (cumulative time to recover)**
- d) acceptability of residual risk**



Issues and Concerns

1. **Navel gazing and the weeds**
 - a. **Most approaches take too long time, dig too deep and can lose momentum and respect**
 - b. **Start with high level assessments and drill down as program matures**
2. **Services/outputs versus tasks/functions**
 - a. **It's not what you do, it's what the client expect**
 - b. **Watch focusing on \$ and systems**
 - c. **80/20 – 20% of your clients generate 80% of the effort (revenues, outputs) - ask your clients!**
3. **Dealing with complicated/conflicting responsibilities**
 - a. **Horizontal management needs requires consensus building techniques (workshops)**



Issues and Concerns (cont.)

4. Realistic, reasonable, acceptable metrics
 - a. Implication of precision that is hard to obtain, timing = ASAP (hours), days, weeks
5. I AM IMPORTANT!
 - a. You are asking the wrong person or the wrong question?
 - b. Top down, facilitates buy in
 - c. It's about timing and dependencies
6. I'm the first priority
 - a. It's not that we don't know what's important we just don't know how we do it (process vs project vs policy)
 - b. Circumstances dictate who's on first and who's on deck – focus on classes of service rankings
7. Worst Case
 - a. What about the all those other more likely situations?

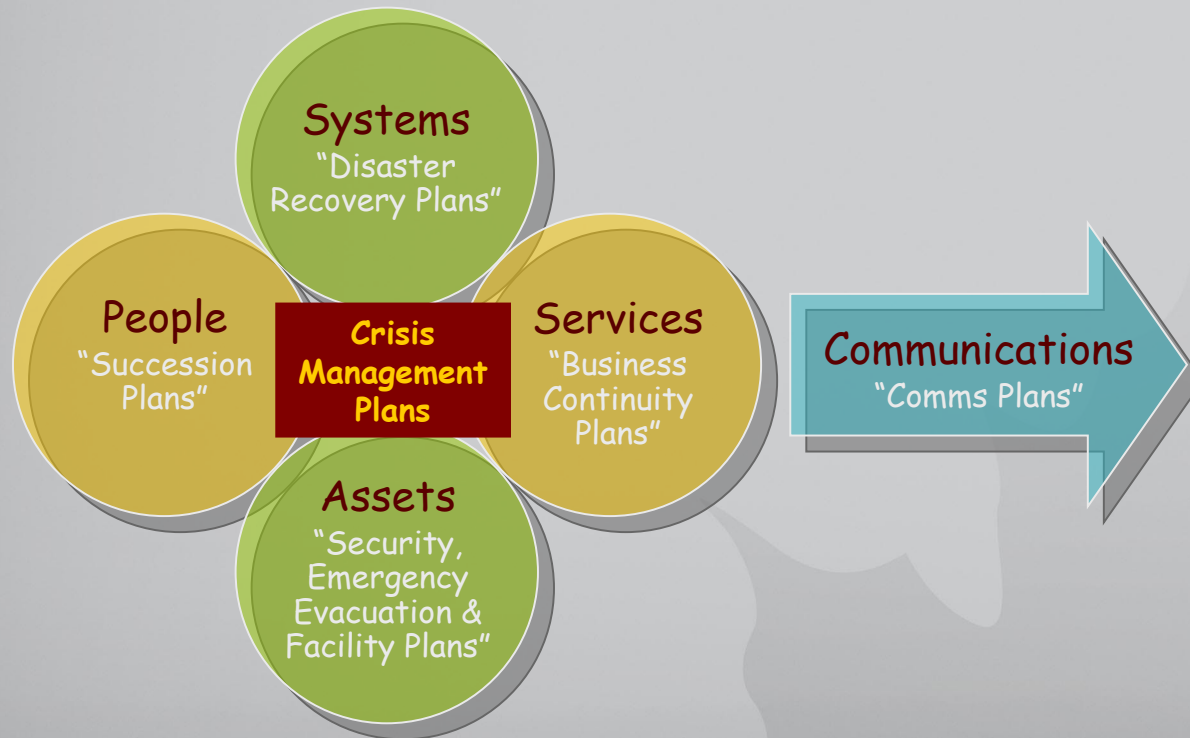


Business Continuity Plans

**... who, what, where,
when**



A Plethora of Plans





General BCP Assumptions

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



General BCP Assumptions (cont.)

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



Anatomy of a BCP

- 1. Who is responsible for decision making (BCP Response Team) and for implementation of response measures (key personnel)?**
- 2. 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)?**
- 3. Where will these services be provided from (alternate site)?**
- 4. Who do we have to contact to let them know the situation (contact lists – employees, clients, corporate services, vendors)?**
- 5. How do we go about recovering services (what steps need to be taken to implement/provide service)?**



On being Prepared

... it's more than just a plan



Preparedness

- 1. Information in BCPs is volatile and needs to be kept current (names, contact information etc.)**
- 2. Situations change and plans, strategies and arrangements to manage risk and ensure the continuity of operations must change also**
- 3. Train, train, train**
- 4. Practice, practice, practice**
- 5. The plans and program should be periodically audited to ensure they meet the needs of the organization**



Training & Awareness

Awareness Sessions, Training Courses, Exercises & Testing, Briefings

- a. all employees (awareness)**
- b. employees of Critical Services (awareness)**
- c. Key Employees (awareness, exercises)**
- d. Response Team Members (training, awareness, exercises & testing)**
- e. BCP Coordinator (training, awareness, exercises & testing)**
- f. Crisis Management Team (training, awareness, exercises & testing)**
- g. Executive Management (briefing, exercises)**



Testing & Exercises

1. Call out testing – time to respond
2. Desk check – plan walk through
3. Simulation – full scale exercise (real time / mock disaster)
4. Procedure verification – business function testing
5. Communications – call out tests, voice system testing
6. IT environment test – reload, restart, alternate site recovery testing (desk check, walkthrough, real time or mock disaster)



The Tabletop

1. You are at home and your phone rings – there has been a fire in the building and it looks bad
2. Now what???

Manage the Incident and deal with the
Consequences!

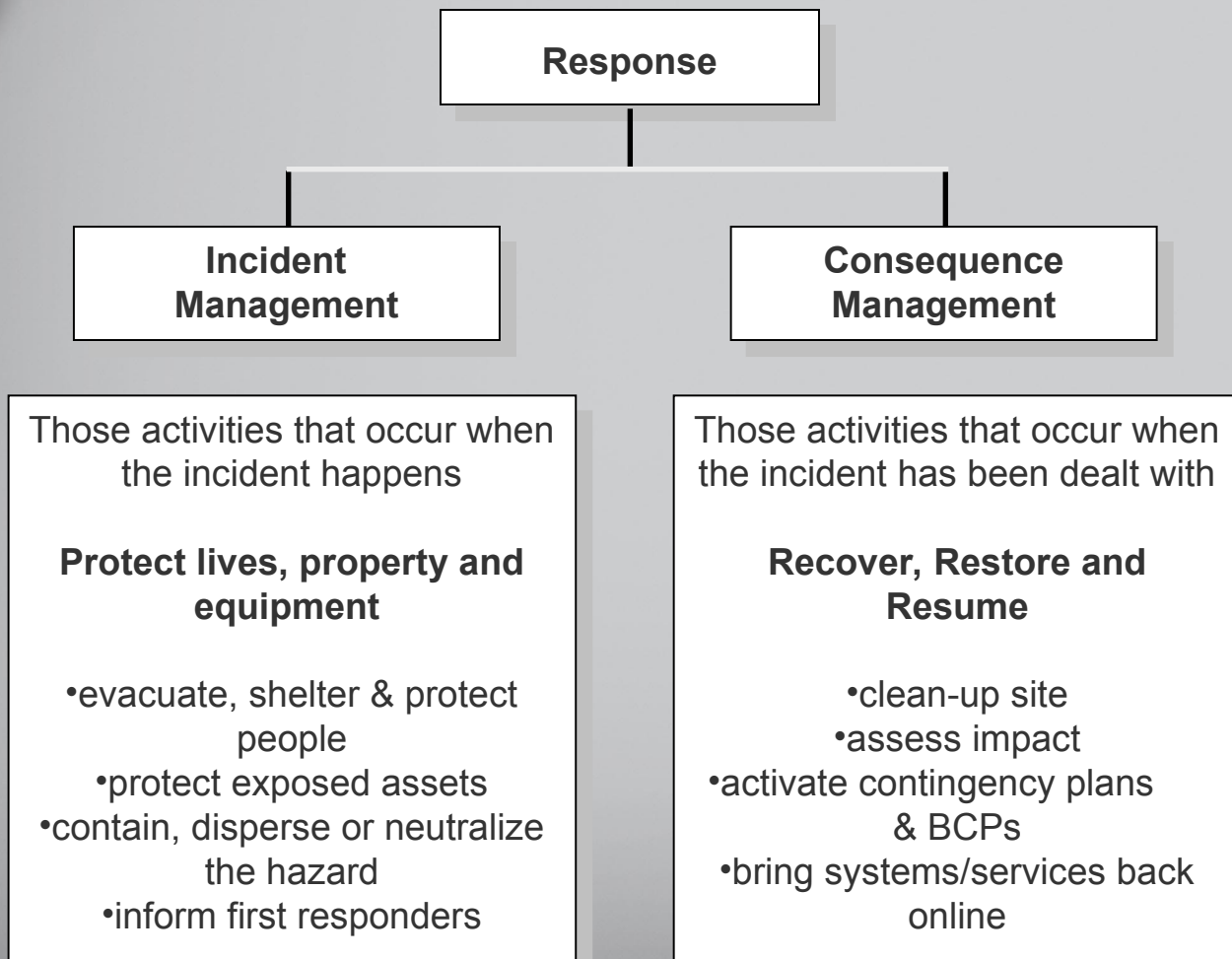


Incident & Consequence Management

**... Managing Service
Disruptions**

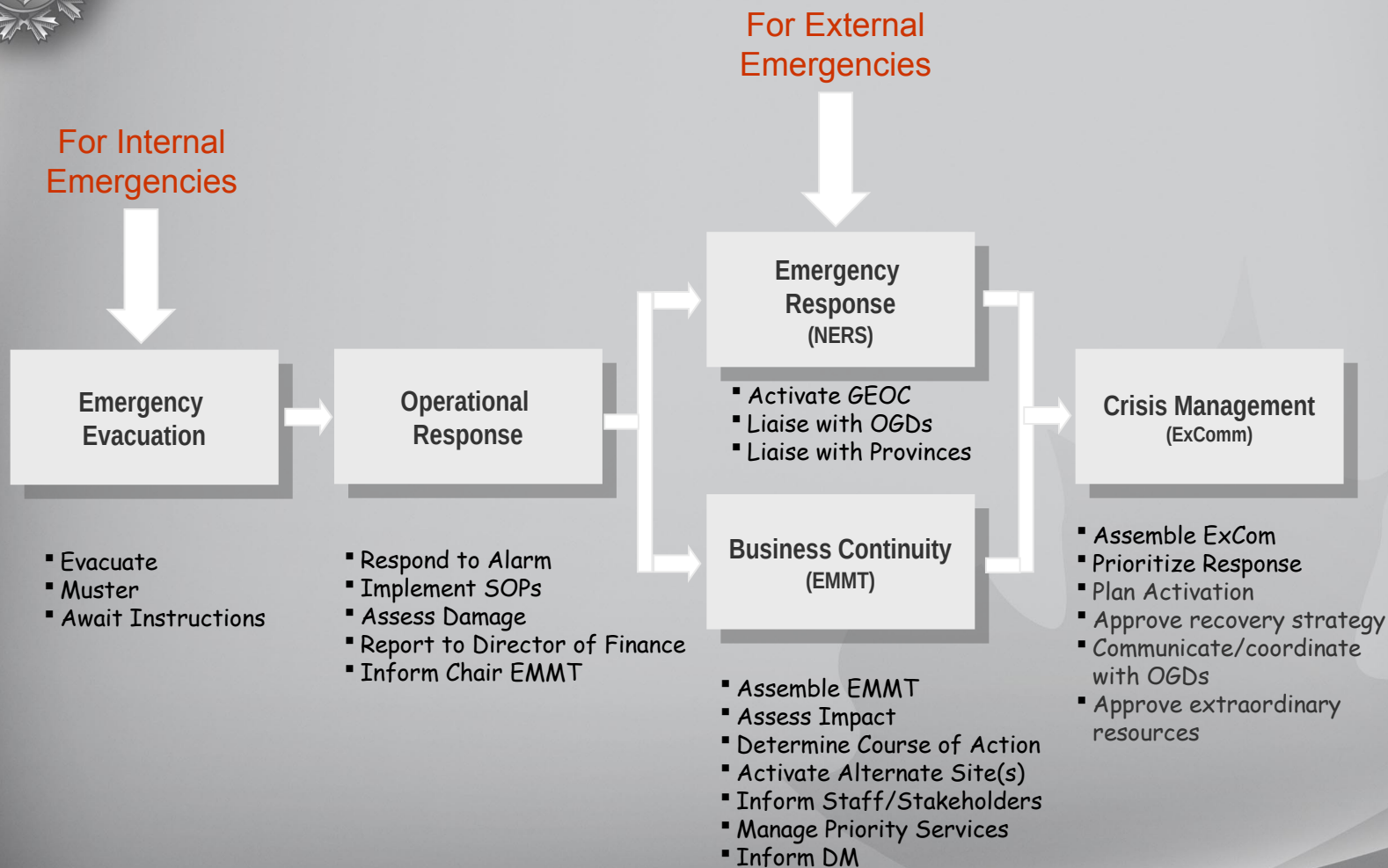


Response Management Regimes



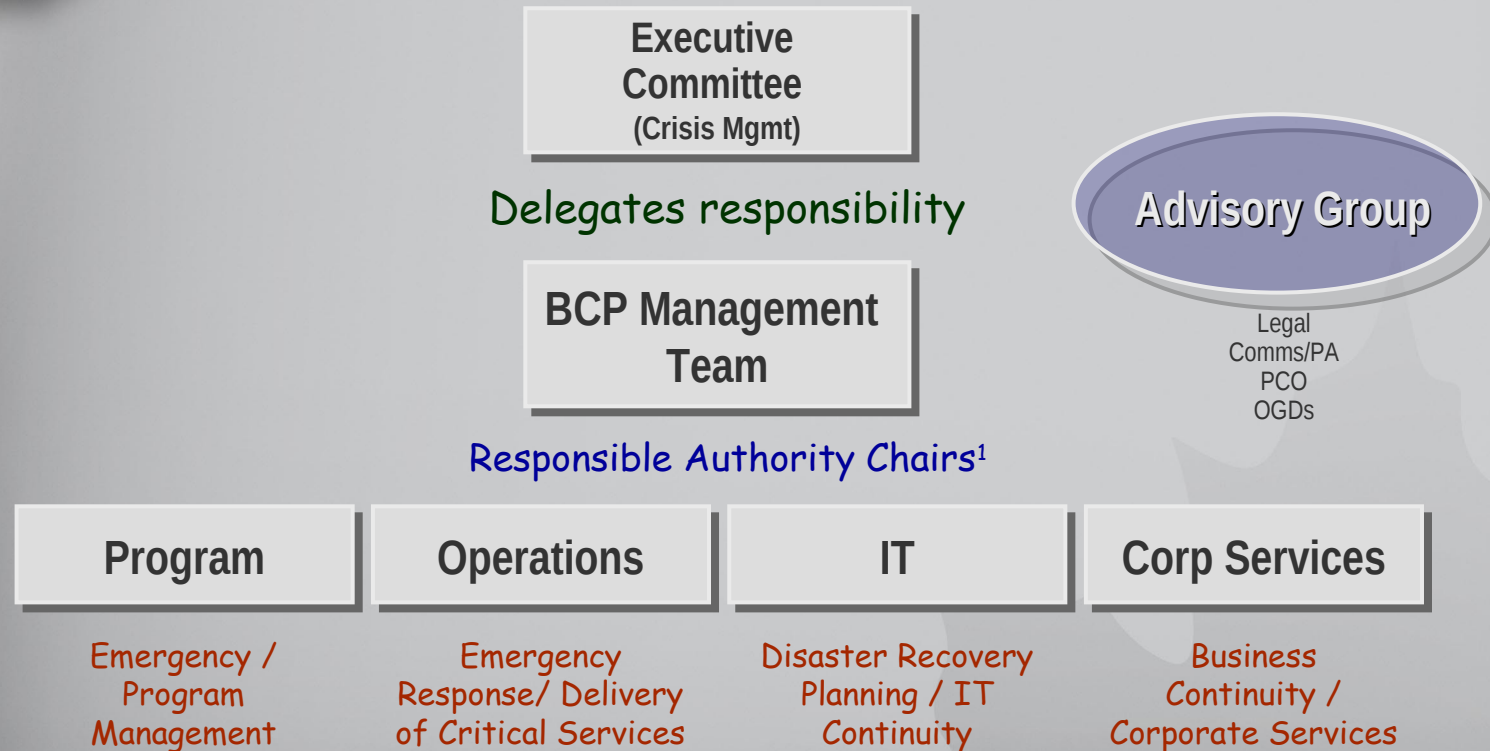


How it all fits together ...





Incident Command and Control



¹ dependant on the nature, extent, severity, impact of the situation the responsible authority could be either a Program Manager (ADM) or L1. Support for managing the incident is then drawn from within the organization as required.



Command & Control

- 1. Establish command and control structure**
- 2. Convene ExCom**
- 3. Conduct ExCom emergency management meeting**
 - a. introductions / remarks**
 - b. situation report**
 - c. questions / clarifications**
 - d. options**
 - e. action planning / communications**
 - f. subsequent meetings**
 - g. closing remarks**



Emergency Operations Centre

1. **General considerations (ensuring operational readiness)**
 - a. primary use as ... security operations centre
 - b. in an emergency becomes Headquarters EOC
 - c. alternate use as a training facility
2. **Design / Layout**
 - a. Command Centre, Emergency Operations Centre
 - b. Media/briefing room, Communications A/V room,
 - c. Quiet Spaces
3. **Location**
 - a. co-locate EOC and command centre
 - b. risk
4. **Resourcing**
 - a. need for people, processes, infrastructure, communications



It's a Wrap!

**... issues for Security
& BCP Types**



Issues for Security & BCP Types

1. **Being prepared – conduct threat and risk assessments and understand what's important**
2. **Mitigating risk – build in redundant, resilient, robust systems/processes and identify alternate sources for requirements**
3. **Working with first responders (fire, police, emergency medical services) – ensure the health and safety of building occupants**
4. **Working with facility managers and with IT – secure the site, mitigate damage**



Issues for Security & BCP Types

1. Working with crisis and emergency managers – logistics and operations support
2. Conducting a damage assessment – determine courses of action
3. Informing management – establish crisis/emergency management team and contact business unit coordinators
4. Activating Emergency Operations Centre – incident and consequence management and control for restoring operations



Questions?

DND/CF BCP Secretariat

**Chantal Cloutier—SJS Dom Plans—CF BCP Lead Planner
613-943-8509**

**Jean-Marc Béliveau—DGCSS—DND Lead BCP Planner 613-
944-6317**

**Sherryl Fraser- SME
613-943-4505**