Agenda

- The Business Continuity Institute (BCI)
- Business Continuity Management (BCM)
- Why should you do this
- How to do it - BCM lifecycle
- Who should be involved - governance
- What you should do – high level view
- Summary
- Q & A and Information

The BCI

The Business Continuity Institute (BCI)

- Headquartered in UK with over 8000 members in over 100 countries
- Chapters in 7 regions – Asia, AU/NZ, Canada, Japan, Nordic, Swiss, USA
- Formal training & formal mentorship for practitioners
- Business Continuity Forum for local practitioners (including Vancouver)
- Publishes Research, Thought Leadership, Continuity Magazine
- BCI Good Practice Guidelines led to BS25999 and later ISO 22301 / 22313

Certification

- Fellow (FBCI) – Senior membership grade awarded for significant contribution to the Institute and the BCM discipline.
- Member (MBCI) – Certified BCM practitioner, min. three years experience and BCI Certificate with merit or other recognized credentials.
- Associate Member (AMBCI) – BCI certificate with at least one year's BCM experience.

Business Continuity Management

What is your "business" i.e. what you do?

- "Business" is not limited to profit making organizations
- Your "business" is the reason your organization* exists
  - *includes; for-profits, non-profits, mutuals, charities, government organizations
  - The majority of critical infrastructure is provided by the private sector

BCM Definition (from BCI Good Practice Guidelines)

Business Continuity Management (BCM) is an holistic process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause.

It provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of key stakeholders, reputation, brand and value-creating activities.

Why BCM – All Organizations

The first rule of business is to "stay in business"

- 25% of businesses do not reopen following a major incident
  - Travellers Insurance / Insurance Institute of Business & Home Safety www.disastersafety.org
- Protect stakeholders: investors & members, employees, customers, suppliers…
- Protect society from the failure of monopolies & critical infrastructure services

Save money

- "If you think safety is expensive, try having an accident" (ditto a business interruption)
- Insurance doesn't fix everything, you can't buy reputation
- Align expenditure with risk (as well as opportunity) – spend only where needed
- Reduce the likelihood of a business interruption – see safety quote above
  - E.g. upgrade the least time-critical workstations first
  - (how do you know these are the least time critical?)

Know how to respond in an emergency

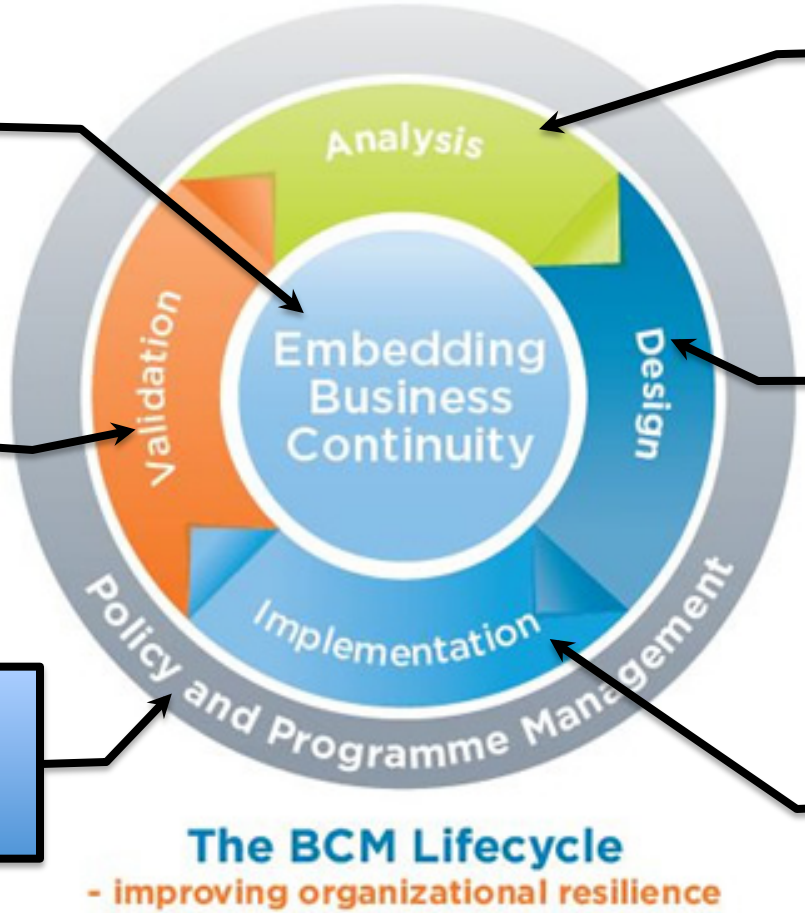
- Create a plan and exercise the plan
- Including what to do next…

Why BCM - Critical Infrastructure

Are you in one of these sectors?
– you may be expected to help in major disasters

Critical Infrastructure	Emergency Response (extended event)	Daily life / The Economy
Energy & Utilities (incl.fuels)	✔	✔✔
Finance (incl. banking)	✓	✔✔
Food (incl. wholesale & distribution)	✓	✔
Government (federal, provincial, local)	✔✔	✓
Health (incl. hospitals & laboratories)	✔✔	✔
ICT (incl. telecomms & broadcasting)	✔✔	✔✔
Manufacturing (incl. "material" suppliers)	✓	✔
Safety (police, fire, ambulance, specialized svcs)	✔✔	✔✔
Transportation (air, marine, road, rail)	✔	✔✔
Water (dams, wastewater / sewage, distribution)	✓	✔✔

The Business Continuity Management Lifecycle*



Awareness &
Training &
Culture

Drills
Exercises & Tests
Plan updates

Governance
Executive Leadership
P-D-C-A

Business Impact Analysis
Risk Assessments

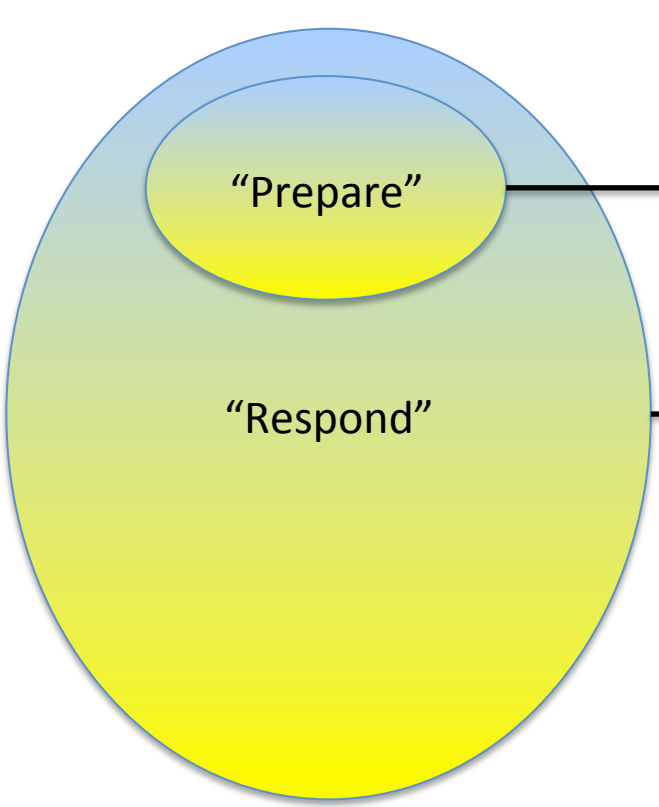
Risk / Cost tradeoff
Accept / mitigate risks
Design controls

"asset protection"
Incident Response Plans
Business Continuity Plans
IT DR Plans

* BCI Good Practice Guidelines

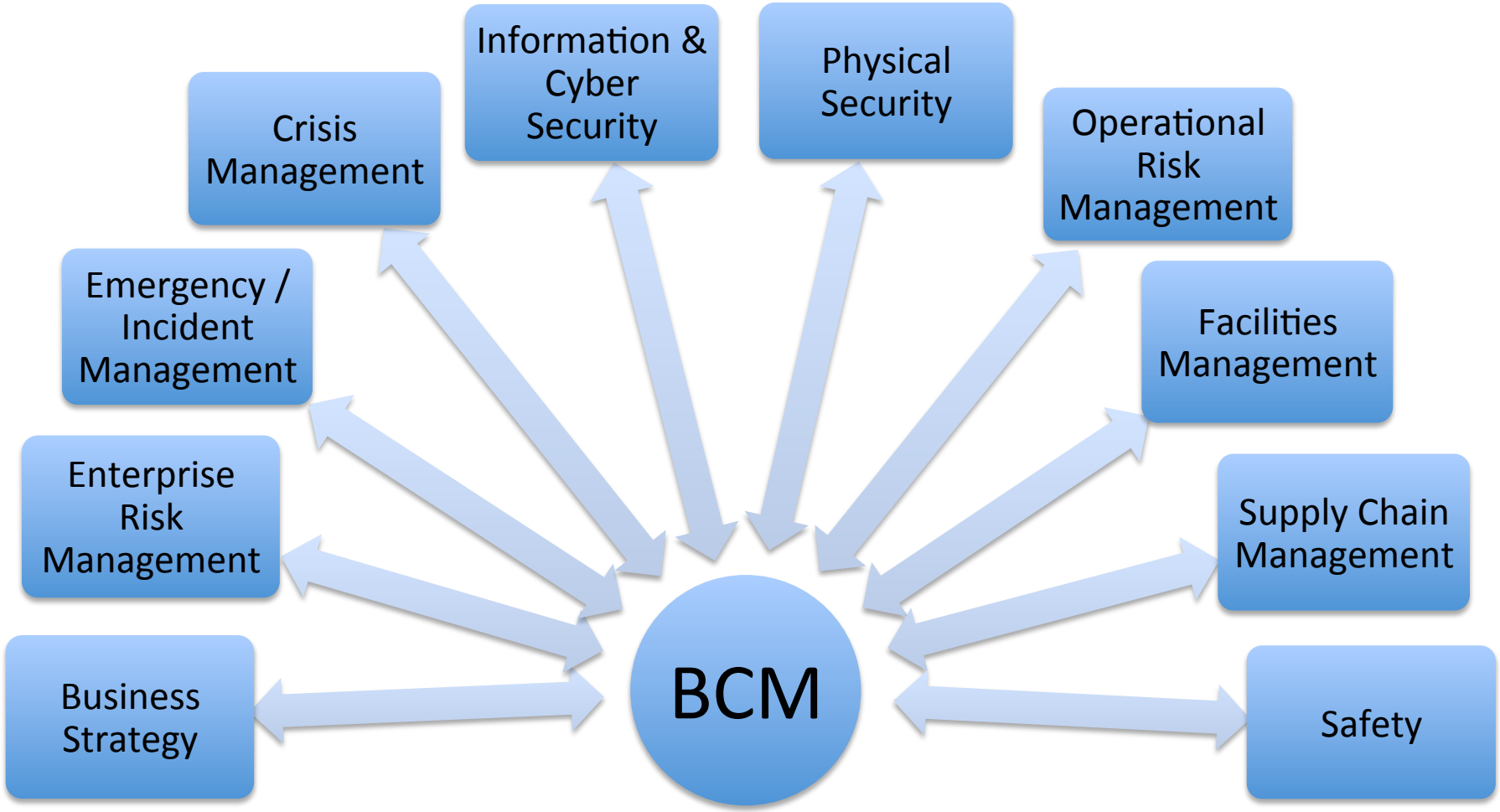
Who - Program Management

Conceptual accountabilities to manage business interruption risks, improve resilience and maintain the ability to respond to major incidents



Policy & Review	**Executive Team**
Risk analyses	Prog. Lead, Risk owners
Approve controls	**Executive Team**
Implement controls incl. arrangements	Risk owners & asset owners
Plan exercises & tests	Prog. Lead
Manage program	Prog. Lead
Exercises & tests	All the above
Execute plans	Dept. staff / responders
Utilize arrangements	Critical suppliers

BCM Touchpoints

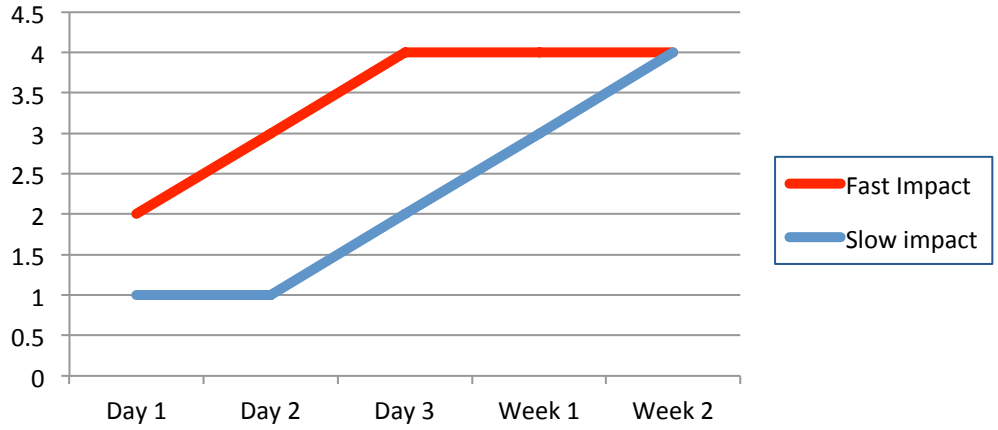


Understanding the business

Business Impact Analysis (3 basic questions)

- What do you DO (business activities)
- What happens if you can't do these things*
- What do you need to sustain these activities (critical resources)

- Impact* as a function of time
- Indicates tolerable outage
- Used to select recovery time objectives



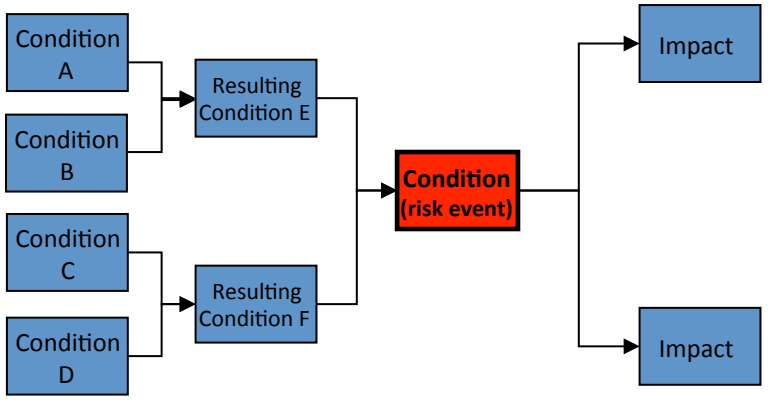
Risk Assessment (for critical resources)

- What hazards are they exposed to & their vulnerability
- Likelihood of occurrence – more on this next…..

* Impact can be : Financial, SLAs, Reputation, Safety, Regulatory… etc.

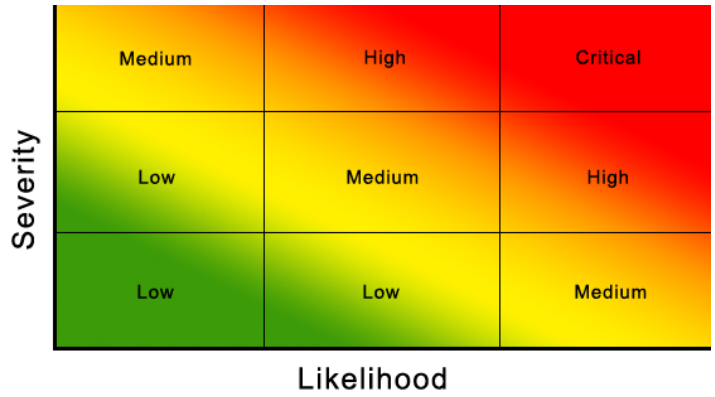
Risk assessments & the probability problem

Theory: Perform a "Bow-Tie" Analysis for each risk event and plot the results on a heat-map



--- Fault Tree Analysis ---

--- Event Tree Analysis ---



Problem: predicting low frequency / high impact incidents (i.e. typical business interruptions)

- You can determine the impact with reasonable accuracy but not the likelihood
- Probabilistic analysis requires accurate data & high certainty (unlikely to have this)

e.g. Predict the likelihood of a fire in your building – consider:

- Insurance data on building fires is useless to you, they have a large portfolio but you do not
- How well was your wiring installed, any cheap extension leads & "personal loads"
- Are you in a multi tenant facility, how are flammables stored?

Who has life insurance & do you know the likelihood of premature death in Canada?

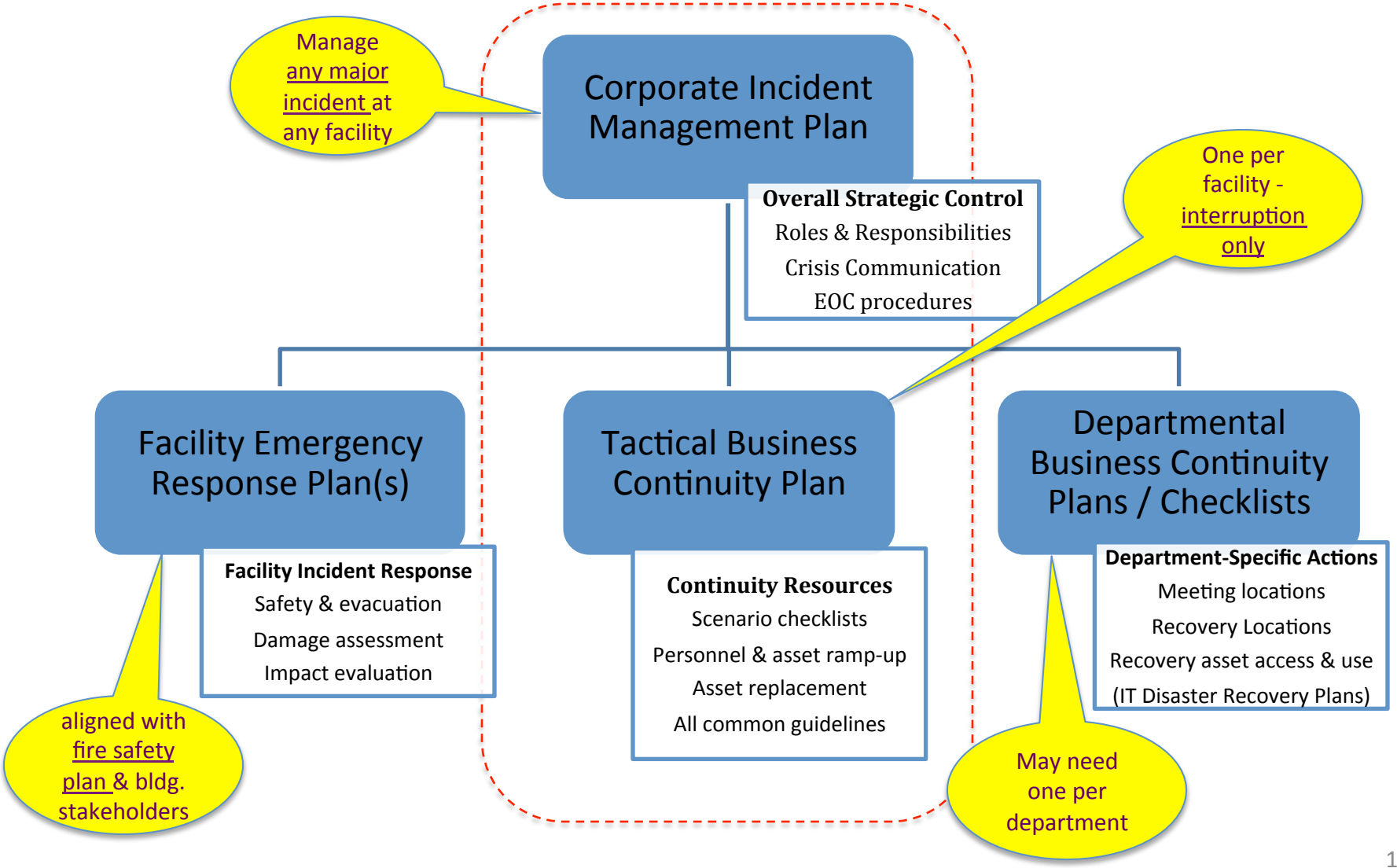
Basic Plan Considerations

- Minimum plan contents
  - Activation Criteria
  - Roles & Responsibilities
  - Priorities - what must be done
  - Recovery resources - what is available
  - Resource replacement – who is responsible (how is in their plan)

- Communication
  - Incident escalation criteria
  - Internal stakeholder communication - Responders & staff
  - External stakeholder communication - crisis communications

- Basic scenarios
  - Facilities failure – fire, flood, denial of access, utility outage....
  - Skills shortage – pandemic, strike, natural disaster, weather …..
  - Information loss – IT failure, critical documents, communications …
  - Supply chain failure – business interruption, logistics, (see skills) …
  - Specialized equipment loss – industrial & testing equipment, vehicles …
  - Inventory loss– destroyed or damaged materials & spares

Concept of Operations / Plans



Drills, Exercises & Tests

Don't trust what hasn't been practiced / tested

- Drills
  - Facility evacuation
  - Earthquake response, including "drop, cover and hold on" (& then what?)
  - Shelter in place
  - Security incidents
- Exercises
  - Incident management team, including crisis communications
  - Facility emergency response teams (in addition to drills)
  - Departmental teams
- Tests
  - IT and other technology recovery
  - Notification systems / call trees
  - Ability to telecommute

Embedding BCM

- Awareness
  - We have a plan? – everyone must know there is a plan & their role
  - Personal preparedness – home & family preparedness
  - Policies & procedures – e.g. critical suppliers, Info security, New risks
  - Campaigns – periodic articles, integrate "shakeout" with BCM
- Training
  - Formal BCM training & certification – BCI certification for program leader?
  - Internal training - Risk owners, steering committee members, "leaders"
  - Drills & exercises & tests – a form of training
- Culture
  - Executive involvement
  - 2 way communication
  - Acknowledge that it "can happen to us"
  - May need to change "the way we do things around here"
  - No blame – mitigate "bystander effect"

Summary

- BCM is a program, not a project
- BCM is enterprise-wide risk management
- Executive involvement is critical
- Both proactive & reactive controls are needed
- Plans should cover:
  - Facility emergency response
  - Incident Management & Crisis Comms
  - Technology recovery
  - Departmental / process recovery
- Leverage leading practices (& standards)
- Use certified practitioners

The BCM Lifecycle
- improving organizational resilience

Where are you in this process – are you ready?

BCI Good Practice Guidelines
www.thebci.org