Business Continuity Management

Stéphane HESSCHENTIER – eBRC - Senior Manager Consulting

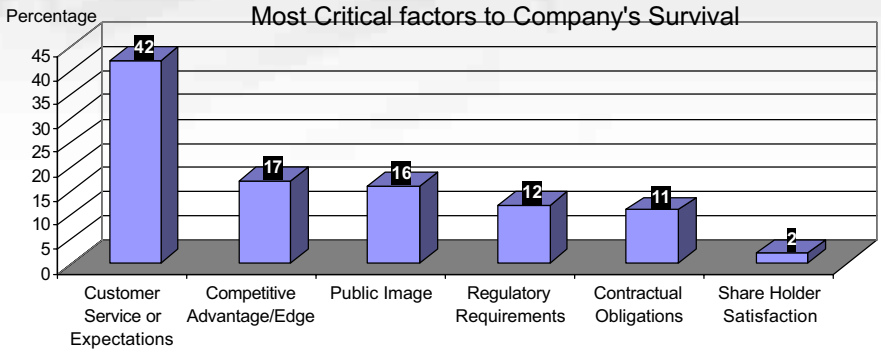
About the speaker…

- Stéphane Hesschentier
- Senior Manager
- Risk & BCM Consulting
- CBCP - MBCI

Agenda

- Introduction to BCM : BCI approach & Other Methodologies
- Understanding the business : BIA & RA
- From BC Strategies to BCM Development
- Testing & exercising BCP

Critical Factors to Company's Survival



Source: Contingency Planning Management (May, 2001)

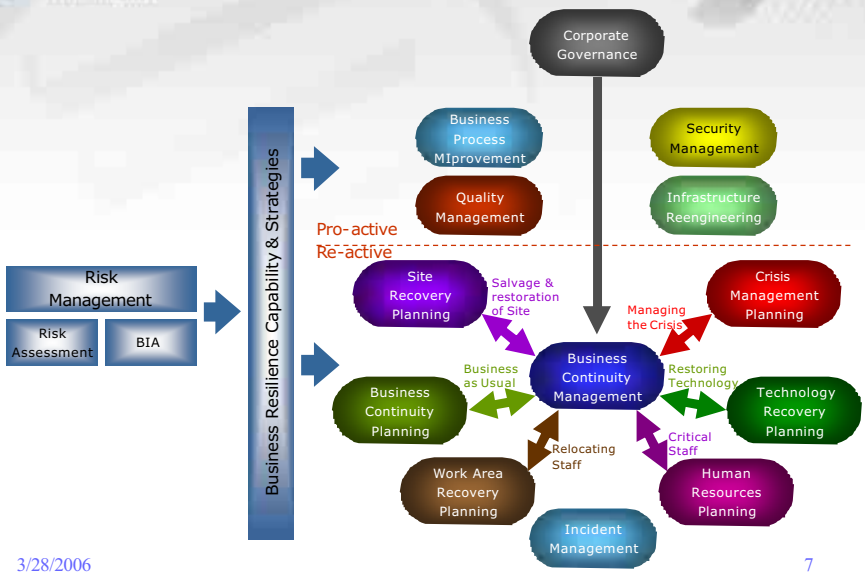
Many Methodologies – 1 approach

- Disaster Recovery Institute International
- Business Continuity Institute
- ITIL
- ISACA
- CRAMM
- IBM
- Deloitte, KPMG, PWC, E&Y,…
- Etc…

BCI Definition vs ITIL Definition

- Business Continuity Management:
  - is a holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience and the capability for an effective response which safeguards the interests of its key stakeholders, reputation, brand and value creating activities.
- ITIL Definition of Continuity management:
  - is the process by which plans are put in place and managed to ensure that IT Services can recover and continue should a serious incident occur. It is not just about reactive measures, but also about proactive measures - reducing the risk of a disaster in the first instance.

BCM Big Picture



BCM Methodology from BCI

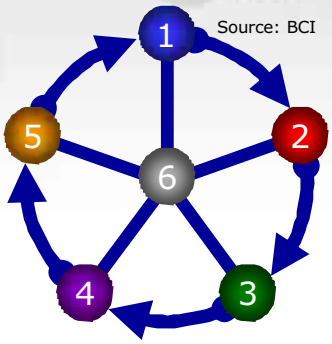
1 Understanding your Business
- Business Impact Analysis
- Risk Assessment & Control

2 Business Continuity Strategies
- Corporate BCM Strategy
- Process Level BCM Strategy
- Resources Recovery BCM Strategy

3 Develop & Implement a BCM Response
- Plans & planning
- External Bodies & Organizations
- Crisis / BCM / Incident Management
- Sourcing / Outsourcing
- Emergency Response & Operations
- Communications
- Public Relations & Media

4 Building & Embedding a BCM Culture
- Education & Training
- Awareness

5 Exercising, Maintenance & Audit
- Exercising of BCM Plans
- Rehearsal of Staff and BCM teams
- Testing of BCM Technology & Systems
- BCM Maintenance
- BCM Audit

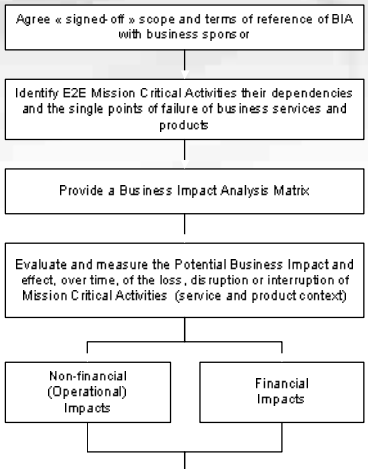


6 BCM Programme Management
- Board Commitment
- Corporate BCM Strategy
- BCM Policy
- BCM Framework
- Roles & Responsibilities
- Finance, Resources, Assurance, Audit
- MIS and Change Management
- Compliance

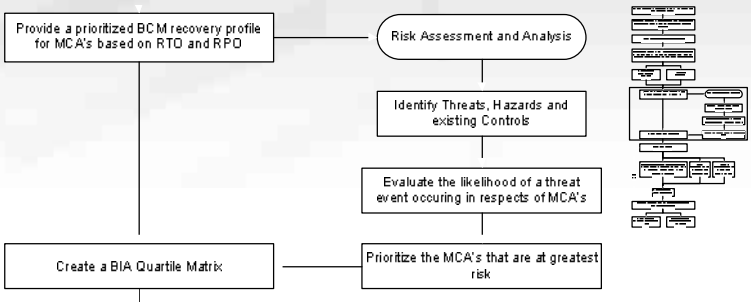
7 Key Success Factors for BCM

1. Develop a BCM Programme Management
2. Understand your Business
3. Design Realistic Business Continuity Strategies
4. Develop and implement a realistic BCM Response
5. The staff is the key to BCM
6. Ensure that the BCM Plan is up to date
7. Be enthusiastic and creative

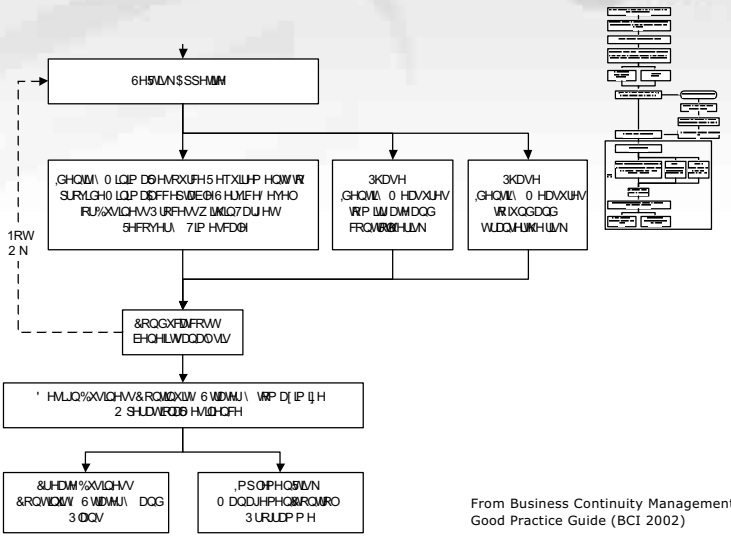
Business Impact Analysis: The BCI approach



Business Impact Analysis: The BCI approach 2



Business Impact Analysis: The BCI approach 3



From Business Continuity Management - Good Practice Guide (BCI 2002)

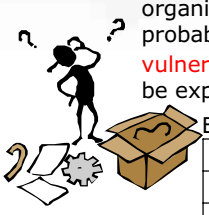
What is a Threat? What is an Asset? What is a Risk?

Threat: a potential cause of an incident that may result in harm to a system or organization.

Asset: anything that has value to the organization.

Risk: the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the probability of an event and its consequence.

vulnerability: a weakness of an asset or group of assets that can be exploited by one or more threats.

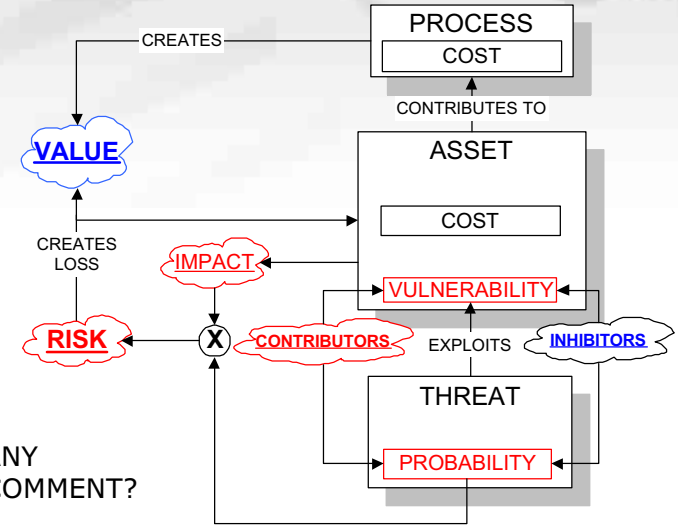


Examples:

Human		Environmental
Deliberate	Accidental	
•Eavesdropping •Information modification •System hacking •Malicious code •Theft	•Errors and omissions •File deletion •Incorrect routing •Physical accidents	•Earthquake •Lightning •Floods •Fire

Source ISO 13335-1

My Risk Model…



ANY COMMENT?

Standardized documentation for Risk Assessment

- Definitions: ISO 13335-1
- Processes & Methodologies : ISO 13335-2
- Integration in Business Continuity Management: BCI Methodology
- Development of Mitigation Solutions: ISO 17799

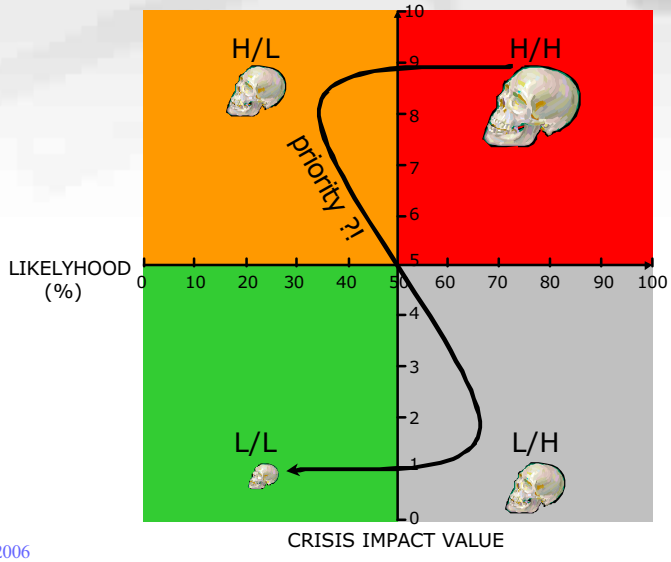
ISO International Organization for Standardization

BCI

Your basic Toolbox to get started…

!!New Naming & Id Nrs!!

Risk Assessment & Business Continuity - Risk Matrix



Many Risk Matrices : Where is the standard?

Incas V2 1999

Probability \ Impact	1	2	3	4
0	0	0	0	0
1	0	1	2	3
2	0	1	3	4
3	1	2	3	4
4	1	2	3	4

IBM

Probability \ Impact	1	2	3	4	5
1	1	1	1	1	2
2	1	1	2	2	3
3	1	2	2	3	3
4	1	2	2	3	3
5	1	2	3	3	3

Yellow Book

Frequency	Severity of Potential Harm/Loss 5 Multiple fatalities	4 Single fatality	3 Multiple major	2 Major injury	1 Minor injury
5= Daily to monthly	25	20	15	10	5
4= Monthly to yearly	20	16	12	8	4
3=1 to 10 yearly	15	12	9	6	3
2=10 to 100 yearly	10	8	6	4	2
1= Less than 100 yearly	5	4	3	2	1

MITRE- Risk Matrix

Probability \	1 Negligible	2 Minor	3 Moderate	4 Serious	5 Critical
0 to 10%	1 L	2 L	3 L	4 M	5 M
11 to 40%	1 L	2 L	3 M	4 M	5 H
41 to 60%	1 L	2 M	3 M	4 M	5 H
61 to 90%	1 M	2 M	3 M	4 M	5 H
91 to 100%	1 M	2 H	3 H	4 H	5 H

Australian Centre for Geomechanics

Rare / Unlikely / Moderate / Likely / Almost certain \ Severity	1	2	3	4	5
1	L	L	L	L	L
2	L	L	L	M	M
3	L	L	M	H	H
4	L	M	M	H	H
5	L	M	H	H	E

MIL-STD-882D

Frequency / Probability	1 Catastrophic	2 Critical	3 Marginal	4 Negligible
Frequent	1 1	2 3	3 7	4 13
Probable	2 2	2 5	3 9	4 16
Occasional	3 4	3 6	3 11	4 18
Remote	4 8	4 10	4 14	4 19
Improbable	5 12	5 15	5 17	5 20

1-5 High
6-9 Serious
10-17 Medium
18-20 Low

Norskhydro - ECC

<0.001 / 0.01 - 0.001 / 0.1 - 0.01 / 1 - 0.1 / 10 - 1 \ Cata	1 Severe	2 Major	3 Med	4 Minor	5
A	H	M	M	L	L
B	H	H	M	L	L
C	H	H	H	M	L
D	H	H	H	M	L
E	H	H	H	H	M

ISO 13335-2

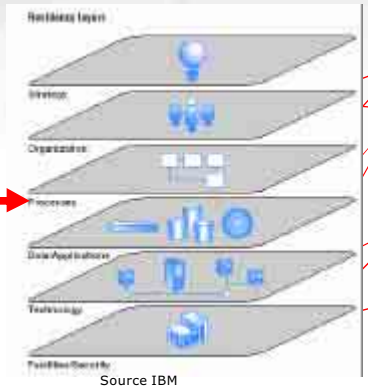
BCI

Etc… Etc… Etc…

Risk Assessment & Business Continuity – How-to

BIA

- Critical Process 1
- Critical Process 2
- Critical Process 3
- …
- Critical Process n



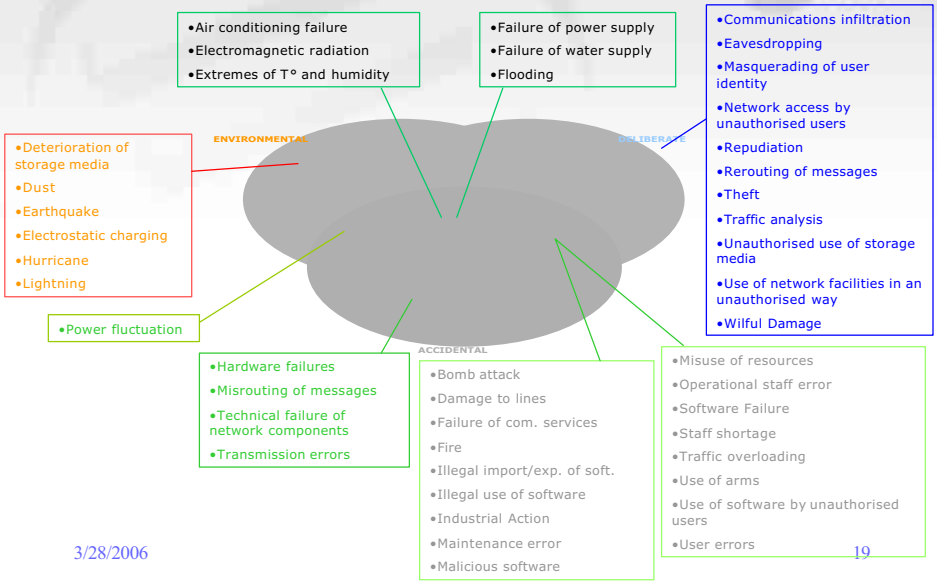
- Threat 1
- Threat 2
- Threat 3
- Threat 4
- Threat 5
- …
- Threat n

Source IBM

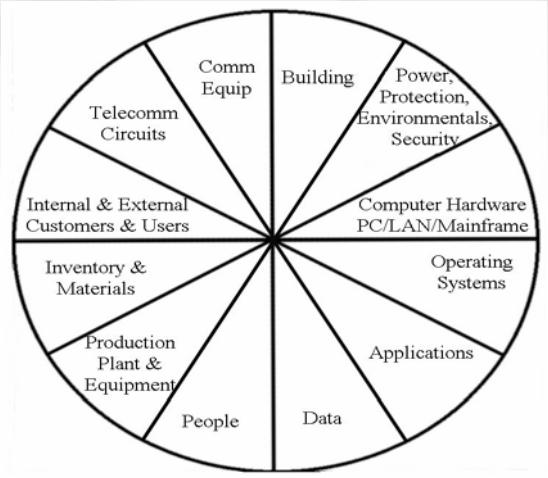
Relevant THREAT

Non Relevant THREAT

Risk Assessment & Business Continuity – Common Threats



Assets to include in the Risk Assessment



Risk Analysis Methodologies in the world

Canada :
- Information security policy make easy
- NSTTI
- STI Canadian Manual
- Guides MG1, MG2, MG3, MG4

UK :
- CRAMM
- BS 7799
- COBRA
- RA Software Tool for Risk Management

Germany:
- IT BASELINE PROTECTION MANUAL

USA :
- BUDDY SYSTEM
- COBRA
- IAM
- IPAK
- RISK ANALYSIS & CONTROL
- RISKETTES

France :
- DSIS
- EBIOS
- INCAS
- MARION
- MASSIA
- MEHARI
- MELISA et MV3
- ORION
- PSI

ISO : Common Criteria / GMITS

OTAN : CM 55-15 / AC/35-D/1006-1027

Source : Cigref 2002 / DCSSI

BCM Strategies

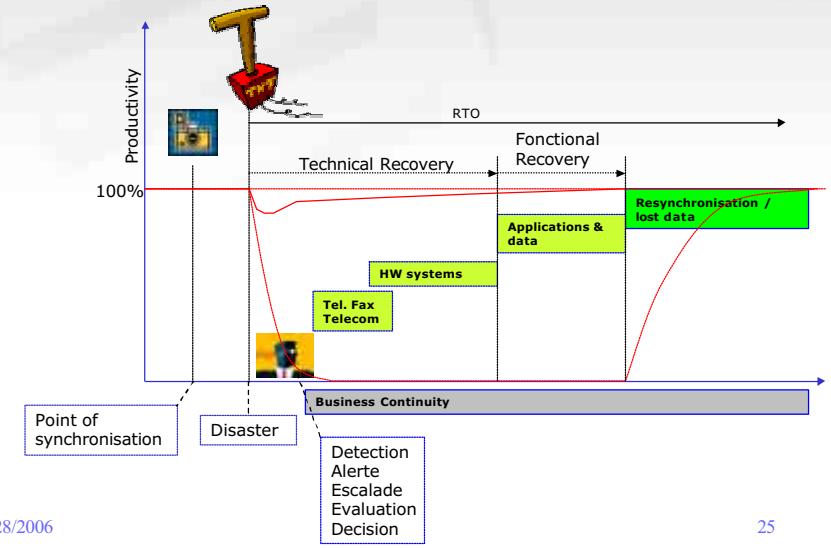
- Your options include:
  - do nothing – in some instances the board may consider a risk acceptable from a business perspective
  - changing or ending the process – deciding to alter existing procedures must be done bearing in mind the organisation's key focus
  - loss prevention – tangible procedures to eliminate / reduce risk
  - business continuity planning – an approach that seeks to improve organisational resilience to interruption, allowing for the recovery of key business and systems processes within the agreed recovery timeframes, whilst maintaining the organisation's critical functions.

How to define BCM Strategies

- You should:
  - identify possible business continuity strategies
  - assess suitability of alternative strategies against the output of the business impact and risk assessments
  - prepare cost / benefit analysis of various strategies
  - present recommendations to sponsors for approval.

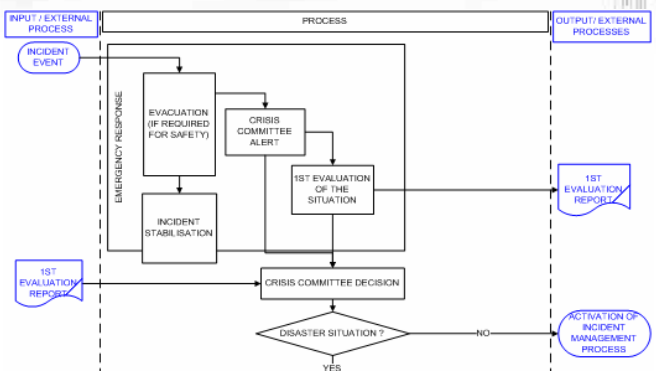
Exemple of BCM Strategy: Recovery Site

Crisis Timeline in practice

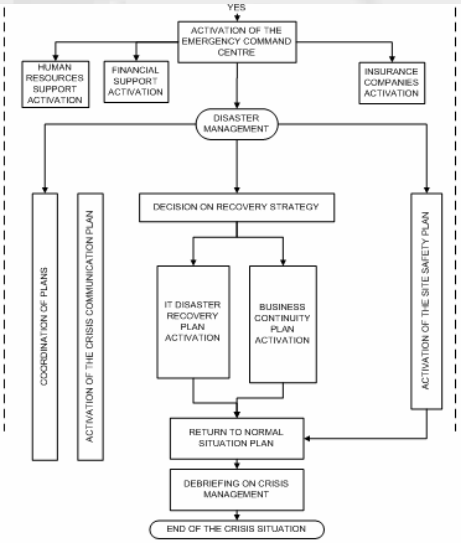


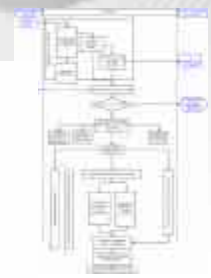
From Crisis Timeline to BCM

- People
- Process
- Technology



From Crisis Timeline to BCM 2





BCM Components

BCI Referential

- Crisis Management Plan (CMP)
- Business Continuity Plan (BCP)
- Disaster Recovery Plan (DRP)

ITIL or BCI Referential

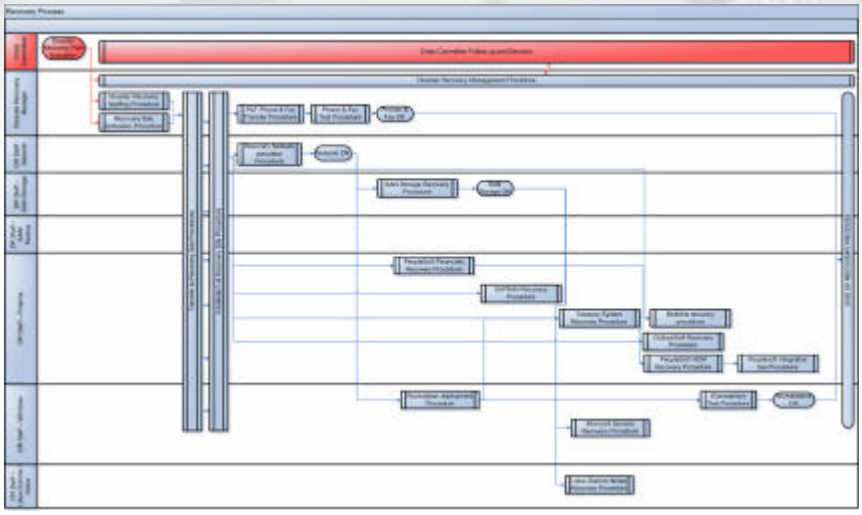
The DRP Table of content

- 1. Abbreviations
- 2. Introduction
- 2.1. Overview
- 2.2. Positioning of the Disaster Recovery Plan
- 2.3. Scope of the Disaster Recovery Plan
- 2.4. What you must absolutely know
- 2.5. Limitations of the document
- 3. Disaster Recovery Plan Solution
- 3.1. DRP solution overview
- 3.1.1. Localization
- 3.1.2. Covered services statement
- 3.2. IT solution Architecture
- 3.3. Contracts and other reference documents
- 3.3.1. Contracts
- 3.3.2. Other reference documents
- 4. Disaster Recovery Flowcharts
- 5. Action Plans
- 5.1. IT Disaster Recovery Manager Action Plan
- 5.1.1. Disaster Recovery Staffing Procedure
- 5.1.2. Recovery site activation procedures
- 5.1.3. P&T Phone & Fax Transfer Procedure
- 5.1.4. eBRC Phone & Fax Transfer Procedure
- 5.2. DR Staff Network Action Plan
- 5.3. DR Staff Notes Action Plan
- 5.4. DR Staff Finance Action Plan
- 5.5. DR Staff SAN Action Plan
- 5.6. DR Staff Microsoft Windows Servers Action Plan
- 5.7. DR Staff Workstation Deployment Action Plan
- 6. Important Contacts List

DRP strategy:

Recoverty Site

DRP on 1 flowchart



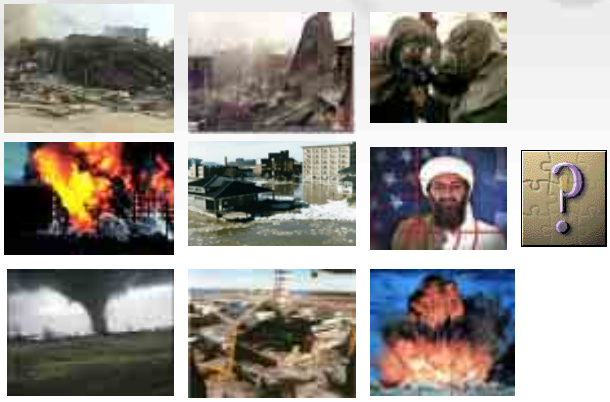
DRP making of : some best practices

- Association of procedures to profiles vs physical persons
- Separation of volatile information & static information (2 DRP volumes)
- Flowcharting vs text
- DRP capability vs resource availability:
  - Avoid useless details / Explain specific tasks
  - 1 expert for writing / 1 IT for revision
- Be pragmatic: no absolute solution / several options
- Be exhaustive: describe the whole process from disaster to return to normal situation
- Technical support very important: help desk required

Crisis Management Main Objectives

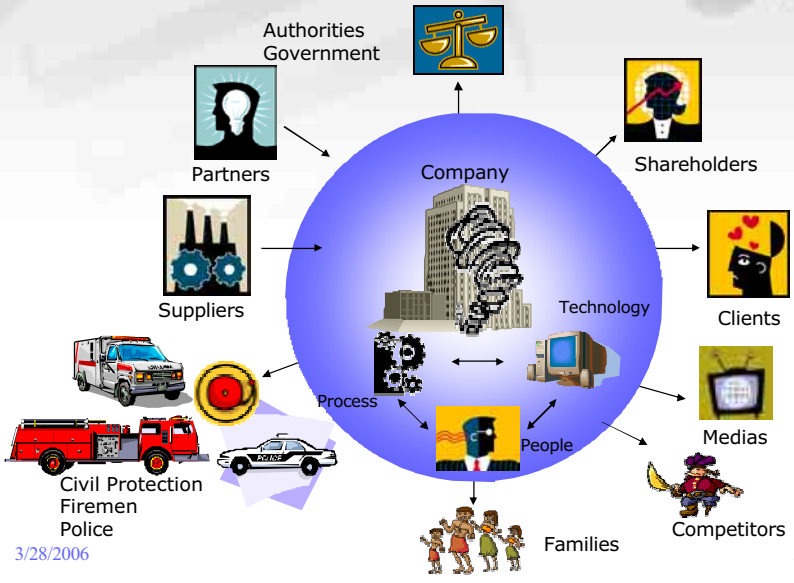
- Management of Disaster Escalation
- Activation of Key Crisis Management Teams & Contracts
- Strategic Decision on CM
- Management & coordination of CM, DRP & BCP Teams
- Management of Communication: internal & external
- Management of Key Supports: HR, Assurances, Finance,…

Relevant scenarios?



If Yes, Crisis Management is a global concern

Global Scope of Crisis Management



Coordination with Authorities - DRII

1. **Identify Applicable Laws and Regulations Governing Emergency Response**
   a) Gather/identify sources of information on applicable laws and regulations
   b) Gather disaster recovery, environmental cleanup, and business resumption requirements
2. **Identify and Coordinate with Agencies Supporting Disaster Recovery and Business Continuity**
   a) Identify statutory requirements for the industry in which the organization participates
   b) Identify and coordinate with public agencies providing disaster assistance (financial and resources); establish liaison procedures
   c) Work with statutory agencies to conform to legal and regulatory requirements
3. **Develop, Implement, and Exercise Plans to Meet Statutory Requirements**
   a) Ensure that plans conform to statutory requirements
   b) Ensure that plan execution is coordinated with public authorities where necessary or required under law (e.g., during a disaster due to terrorism, bombing, or other criminal activities that require intervention by public authorities)
   c) Periodically review liaison procedures

EMERGENCY RESPONSE and OPERATIONS

1. Identify Potential Types of Emergencies and the Responses Needed (e.g., fire, hazardous materials leak, medical)
2. Identify the Existence of Appropriate Emergency Response Procedures
3. Recommend the Development of Emergency Procedures Where None Exist
4. Integrate Disaster Recovery/Business Continuity Procedures with Emergency Response Procedures
5. Identify the Command and Control Requirements of Managing an Emergency
6. Recommend the Development of Command and Control Procedures to Define Roles, Authority, and Communications Processes for Managing an Emergency
7. Ensure Emergency Response Procedures are Integrated with Requirements of Public Authorities

Components of Emergency Response Procedure

- Reporting procedures
  - Internal (escalation procedures)
  - External (response procedures)
- Pre-incident preparation
  - By types of disaster
  - Management continuity and authority
  - Roles of designated personnel
- Emergency actions
  - Evacuation
  - Medical care and personnel counseling
  - Hazardous material response
  - Firefighting
  - Notification
  - Other
- Facility stabilization
- Damage mitigation
- Testing procedures and responsibilities

Dos and Don't in Crisis Communication

- During an emergency **DO**:

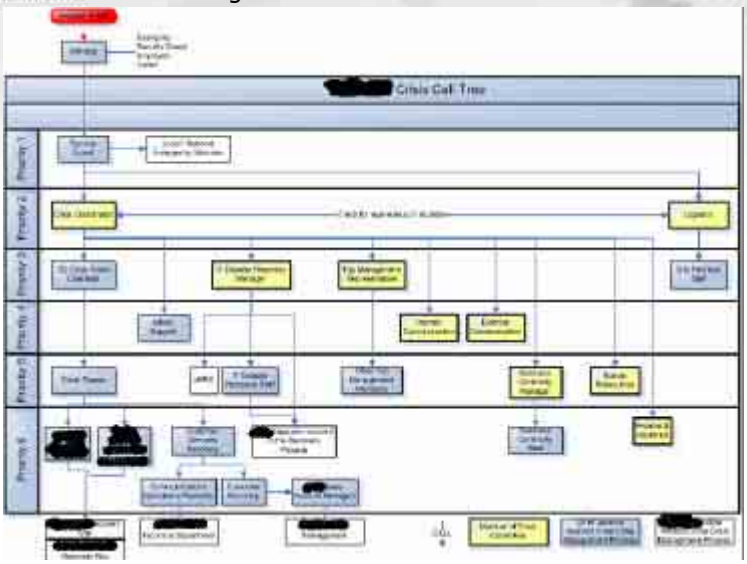
1. Release only verified information.
2. Escort the news media everywhere on the emergency site.
3. Have a designated spokesperson.
4. Keep accurate records and logs of all inquiries and news coverage.
5. Learn media deadlines and try to meet them.
6. Provide equal opportunities and facilities for print and electronic media.
7. Have a clear idea of what can and cannot be released.
8. Carefully coordinate planning and implementation of public relations activities with other aspects of the comprehensive emergency plan.

- During an emergency **DO NOT**:

1. Idly speculate on the causes of the emergency.
2. Speculate on the resumption of normal operations.
3. Speculate on the outside effects of the emergency.
4. Speculate on the dollar value of losses.
5. Interfere with the legitimate duties of news people.
6. Permit unauthorized spokesperson to comment to the media.
7. Attempt to cover up, or purposely mislead the news media.
8. Place blame for the emergency.

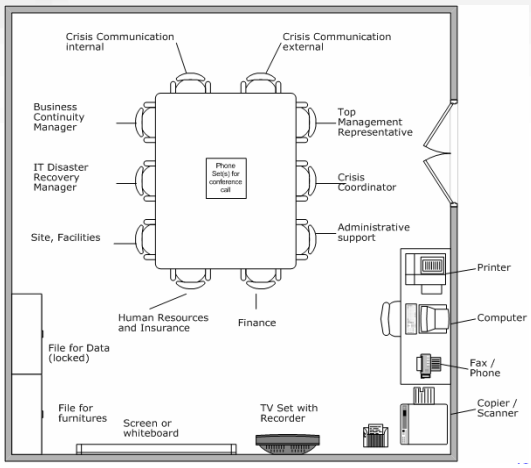
CMP Table of content

Crisis Management Plan Call tree



Emergency Command Centre

A key infrastructure for Crisis Management



CMP making of: some best practices

- Keep it simple: Generic global scenario vs. hundreds of scenarios
- Key Success Factor of CM=Human Resources:
  - Be flexible
  - Do not rely on 1 specific person
  - Human loss to be considered
  - Disaster => Human impact => Low efficiency
- Facilitiation of CM (options) vs. CM Process
- No ambiguous situation
- Give the possibility to take good decisions in bad situations: what is a disaster?
- Key Success Process of CM = Communication

BCP Table of Content

- Next Step…Not yet implemented for the client
- What should be included in the document- Table of Content:
  - SECTION 3: Business Continuity Manager
  - 3.1: Role & Responsibilities
  - 3.2: How to Use this Plan
  - 3.3: Supporting Staff
  - 3.4: Standby Locations
  - 3.5: Public Relations
  - 3.6: Actions for Business Continuity Manager
  - 3.7: Key First Priority
  - 3.8: Contact Lists
  - 3.9: Vital Materials List
  - 3.10: Business Continuity Manager: Equipment & Software & Timescale for Provision
  - 3.11: Business Continuity Manager Log
  - …
  - SECTION 6: nn Team Plan
  - 6.1: nn Team Role & Responsibilities
  - 6.2: How to Use this Plan
  - 6.3: Staffing
  - 6.4: Standby Locations
  - 6.5: Public Relations
  - 6.6: nn Team Action Plan
  - 6.7: Key First Priority
  - 6.8: Contact Lists
  - 6.9: Vital Materials List
  - 6.10: Equipment & Software & Timescale for Provision
  - 6.11: nn Team Business Continuity Activity Log

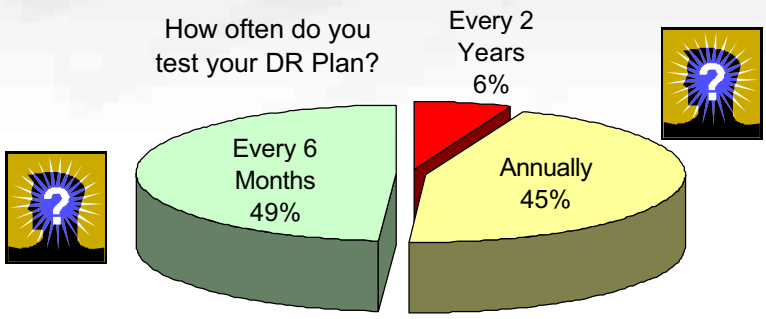
BCP making of : Best Practices

- Several strategies vs. 1: no perfect system
- Degraded mode is inevitable: explain how
- Priorities Managed / Conflicts reported to Crisis Committee
- For each BC Process: Who, When, What, How, Where, With ?
- Do not explain normal job
- Key Success Factor: Human Ressources (Again)

BCM Automated tools: Many suppliers

Alertcast Emergency Notification
Advanced Process Solutions, Inc.
Binomial Phoenix
BRProactive, Inc. A Business Recovery and Services Company
STROHL SYSTEMS
Business911 International, Inc.
BUSINESS PROTECTION SYSTEMS, INC.
RSM McGladrey, Inc
CSCI Business Continuity Planning
GSA Disaster and Business Recovery
Persson Associates DRP Since 1985
RECOVERY PLANNER
PRESAGE CORPORATION
SUNGARD Availability Services
DISASTER RECOVERY
VERITAS
OFFICE SHADOW

BCP Testing Statistics

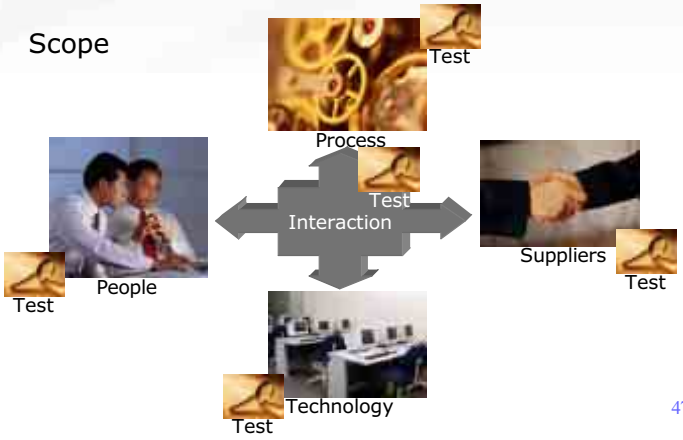


Definition & Scope

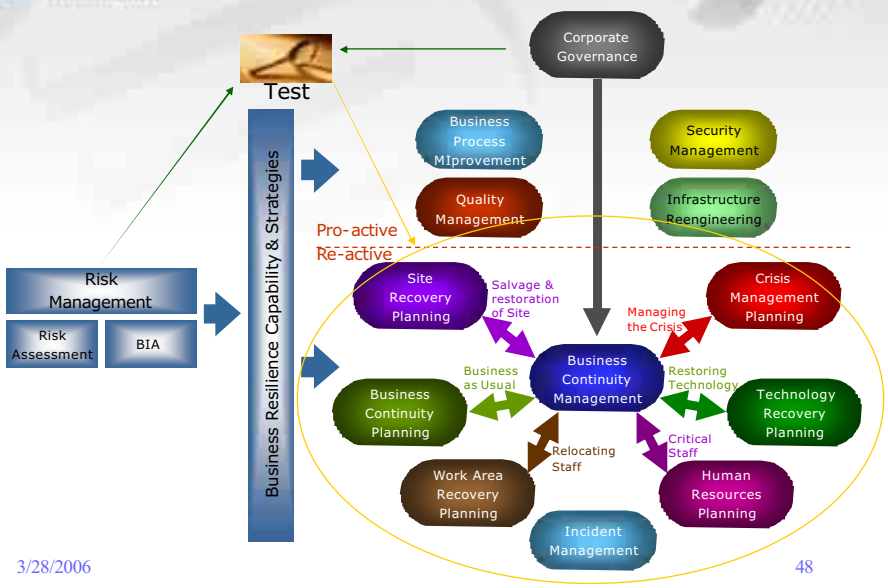
Definition:

- execute an exercise.
- Control with operations that a system is well functioning

Scope



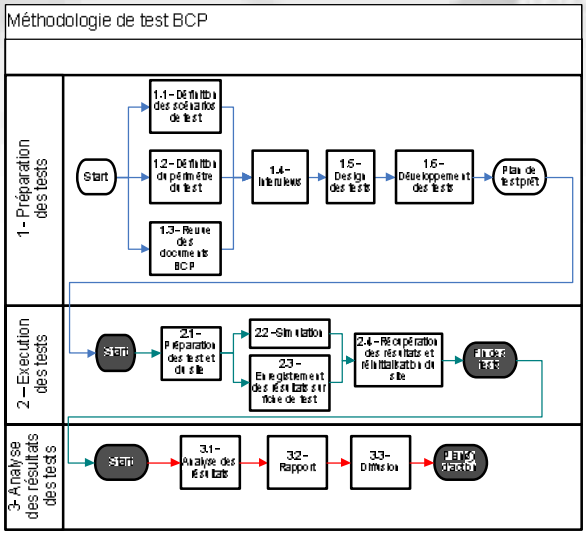
BCM Testing Scope & BCM Big Picture



Types & Goals of BCP Tests

- Types of tests:
  - Walkthrough Tests
  - Procedures Verification Tests
  - Simulation Tests
  - Real Conditions Tests (Careful)
- Goals:
  - Verify feasibility of Business Resilience Processes
  - Verify performance
  - Measure results : Recovery time, % activities recovered, Nb of errors
- Logical Sequence of tests:
  - Tests on paper (Process) & Tests of Knowledge (Staff) & Tests of equipment (Systems/technology)
  - Scheduled Simulation Tests : Limited/Large Scope
  - Unscheduled Simulation Tests

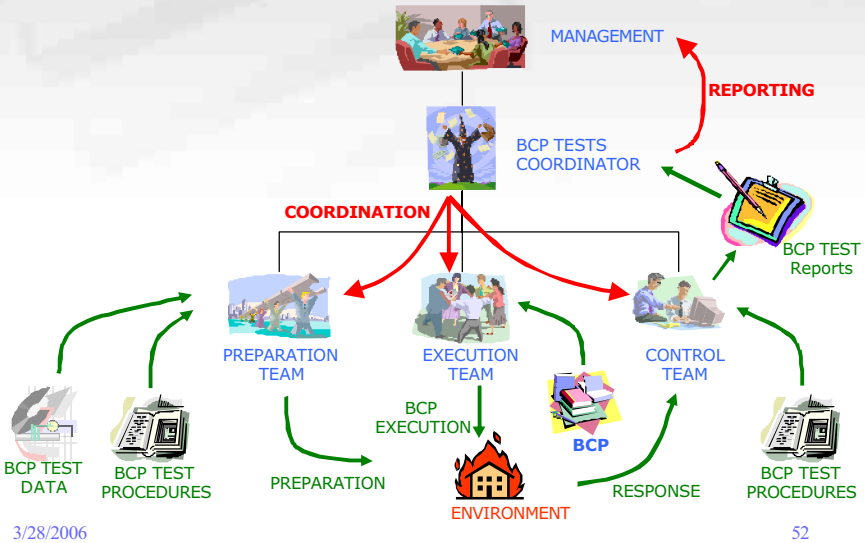
Example of BCP Testing Methodology



Prepare Simulation Tests

- Define a Crisis Scenario
- Create a Simulation Environment
- Establish a Test Protocol
- Define Test Criteria
- Define conditions for: Validation, Interruption, Derogation
- Define Test triggers
- Define who is involved in Tests
- Create Test Forms : Recording & Guidance

Implement a Test Organization



Simplified Test Form

Name of the Test Procedure	Reference	Date: 11/11/2002 Written by: S.Hesschentier

OBJECTIVES OF TESTS

Scenario *Include here the description of the scenario*	Components of the BCP involved

TESTS ORGANISATION

Coordination by: BCP Execution by: Controls by:	Localization: Resources:

TESTS EXECUTION

Start:	End:	Id:

	BCP: Module	by:	Test: Control	By:	Result		Status
					Target	Real	☹ 😐 ☺
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							

Comments:	Status of the Test Procedure: ☹ 😐 ☺ Next test on:

Questions & Answers

References

- http://www.drii.org
  Website du Disaster Recovery Institute International
- http://www.thebci.org
  Website du Business Continuity Institute
- http://www.ebrc.lu
  Website of eBusiness & Resilience Centre
- http://www.contingencyplanning.com
- http://www.drj.com
- http://www.globalcontinuity.com

Thank you for your attention

For additional information:

- eBRC – Stéphane Hesschentier
  - Tel: 26 06 1
  - Email: stephane.hesschentier@ebrc.lu
  - Web: http://www.ebrc.lu