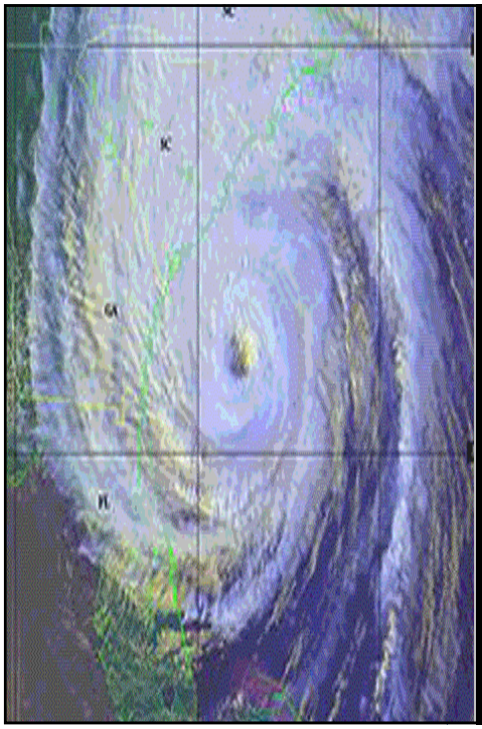


BCM from a Consultant's Perspective

by

Jacques A. Heide

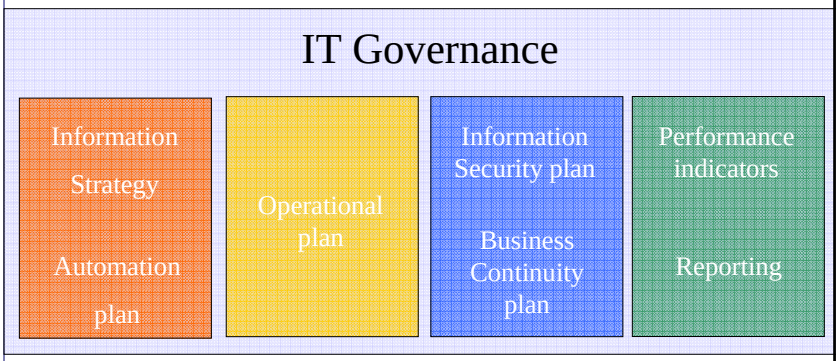
Curaçao, 24 June 2010

Central Bank N.A.

Goal: *BCM from a consultant's view*

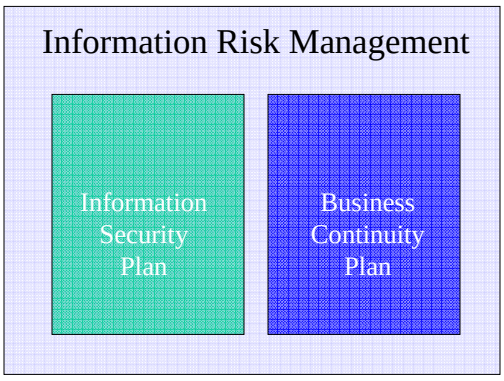
1. Insight in how to approach BCM (*best practices*)
   Source: Provisions guidelines Business Continuity Management of the Central Bank and
2. (of course) how consultants can help

Governance of information provisioning



3

Helicopter view on information security



4

Simplified approach

- Structured, by means of a methodology
- Mobilize key personnel
- Analyze (daily) business operation
- Assess risks
- Perform a business impact analysis (BIA)
- Define countermeasures
- Plan: disaster, rollover, recovery, resumption, etc.
- Test
- Maintain

5

Risk management

Are the risks - with business continuity in mind – mitigated properly?

- Timely, deadline may be fixed?
- Completely, no surprises?
- Effective, according to expectations?
- Efficient, at acceptable costs?

6

Approach risk management

- Assessment
  - Inventorize
  - Analyze impact (BIA)
- Plan
  - Define countermeasures
  - Conduct reviews
- Control
  - Execute and monitor countermeasures

7

Analysis

8

Potential threats

- Nature (storm, lightning, floods)
- Technical (software- & hardware bugs)
- Environment (fire, explosion, power, temperature, humidity, flooding, smoke, ashes, dust, construction errors, vandalism, chemical spills, air or sea disasters)
- People: unintentional (negligence, untrained, inexperienced, errors)
- People: malicious (theft, misuse, hacking, virus, strikes, vandalism, bomb threats, sabotage)

9

Lessons Learned from Disasters (1)

Origin: organized attack

10

Lessons Learned from Disasters (2)

Origin: failed smoke detector (*system failure*)

11

Operational threats

Threat to business continuity:

- Indirectly by interruption of business processes
- Directly by disruptions to the infrastructure
  - Technical failures
  - Vandalism, sabotage
  - Accidents, e.g. fire
- Directly by enforced measures, e.g. politics

12

Risk analysis

- Inventorize & quantify threats
- Inventorize & quantify IT components
- Inventorize & quantify vulnerabilities
  - Which processes should stay operational?
  - Which is het *minimal acceptable service level* (MASL)?
  - Which *downtime* is acceptable?

13

Chance-Impact matrix

Impact / Chance	Low	Medium	High
High	Significant risk	Big risk	Maximum risk
Medium	Minimum risk	Significant risk	Big risk
Low	Minimum risk	Minimum risk	Significant risico

14

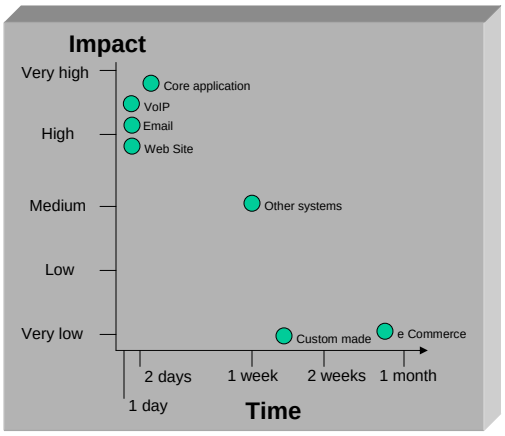
Impact matrix

Risk	Chance	Financial loss	Ungovernable	Total risk
Telecommunication interupted	25%	10	10	25
Electric power interupted	10%	10	5	5
Air- or sea service interupted	1%	2	3	0.06

Total risk = Chance x Financial loss x Ungovernable, 1= low, 10 = high

15

Example impact analysis



Impact against duration of the interruption

16

Mitigation of risks

- Preventive actions
  - Minimize chance of occurrence
- Reduce impact of materialized problem
  - Define contingency
  - Contractually outsource help
  - Financial insurance against loss

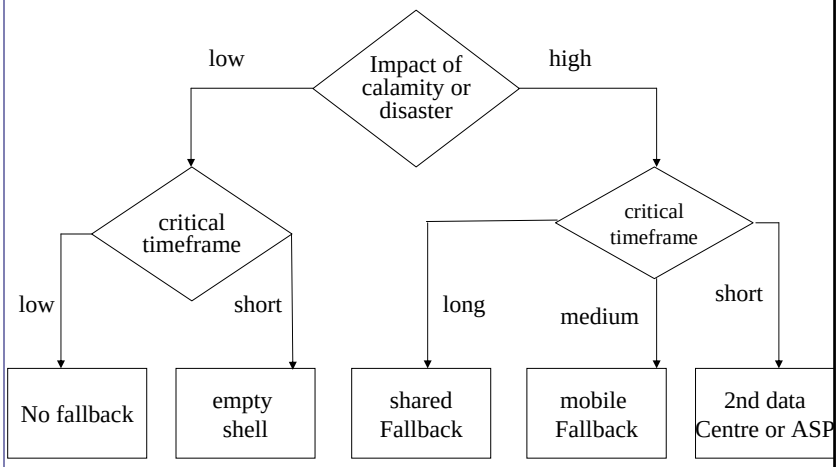
17

Countermeasures

- Define countermeasures
  - Brainstorm
  - Best practice countermeasures (2nd datacenter?)
- Choose countermeasures
  - Security
  - Cost / benefits
  - Acceptable loss (data, time, *throughput*, etc.)
  - Location
- Implement countermeasures

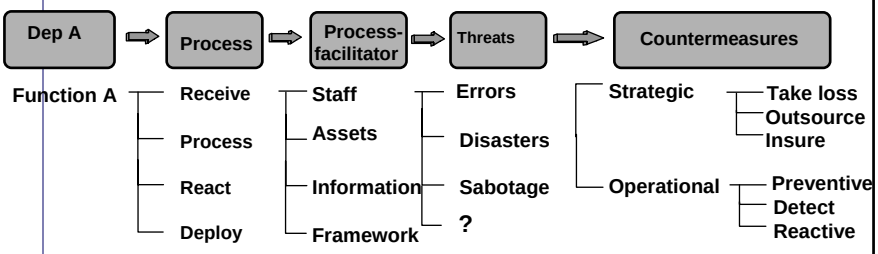
18

Choice tree @ disasters or calamities



19

Operational risk model



20

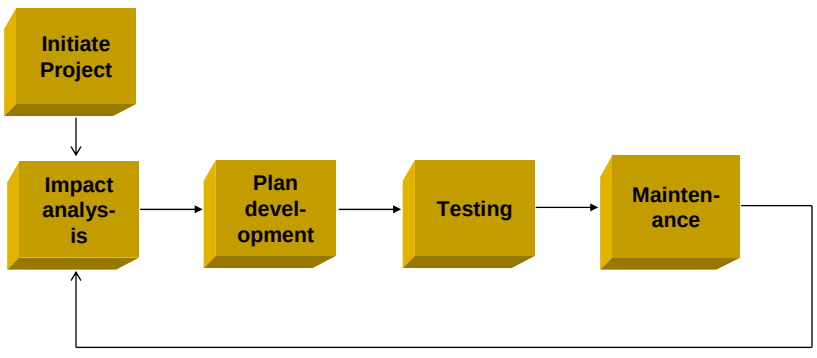
BCM

Business Continuity Management (BCM) leads to:

- continuity of business processes
- during a certain period
- on a defined acceptable level
- under uncertain conditions

21

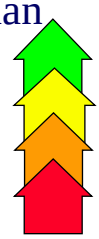
5 steps leading to a BCP



22

Various plans

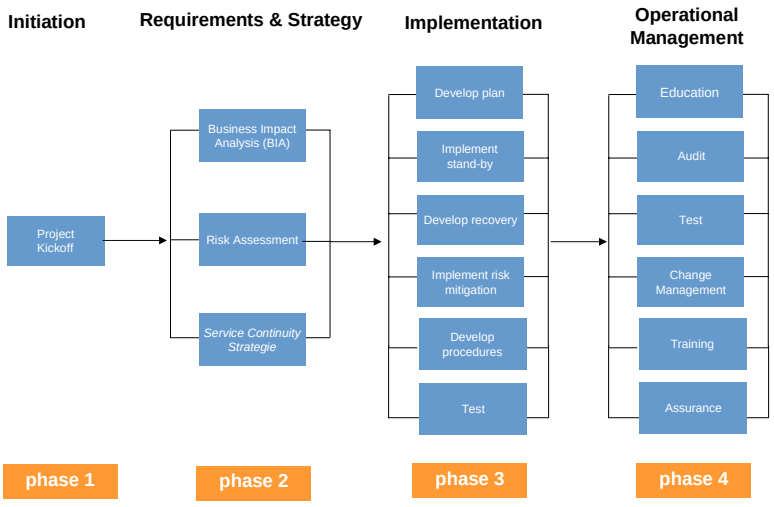
- *Disaster recovery* plan
- *Resumption* plan
- *Recovery* plan
- *Emergency* plan
- *Contingency* plan
- *Business continuity* plan



- *Avoidance* (BCP)
- *Contingency*
- *Crisis Management*
- *Disaster Recovery*

23

Business continuity planning lifecycle



24

Business continuity plan

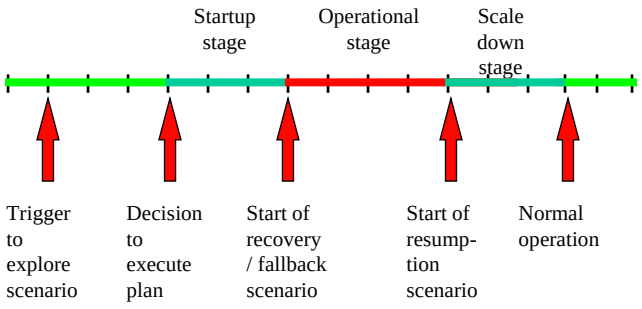
- Operational continuity is key
- Risk management is essential
- Strategic (not technical)
- Custom made (!)
- Carried by the organization
- Never finished
- Always necessary

Contains:

- Procedures
- Instructions
- Contracts
- List of needed assets
- Reserved spaces / capacity
- Crisis organization
- ...

25

BCP stages



26

BCP example solutions (1)

	Preventive actions	*Disaster Recovery*	*Fallback scenarios*	*Cushions*
Info systems	Procedures Maintenance	Recovery procedures Backup procedures	Fallback Alternative systems	Reconstruction Insurance
Com-munication	Communication plans		Double configuration	
Transport & infra.	Contracts Stand-by capacity	Risk analysis Instructions	Fallback procedure	Insurance
Logistics	Contracts Agreements with lsuppliers	instructions	Alternative suppliers	Buffering

→ →

27

BCP example solutions (2)

	Preventive actions	*Disaster recovery*	*Fallback scenarios*	*Cushions*
Production	Maintenance	Instructions	Fallback	Insurance
Facilities	Maintenance Security Inventory	Instructions ,	Fallback	Insurance
Personnel	Backup Key figures Temps	Instructions	Temps	
Finance	cashflow planning	Instructions	DLA Alternative cash	

28

Remarks

1. BCM mandatory by Supervisor
2. Business (read operational) continuity is mandatory for clients, personnel, shareholders and other stakeholders
3. Complex matter
4. Curaçao has its share of possible high impact threats: weather, flooding, power, telecommunications and personnel
5. There is help! Supervisor, consultants, suppliers, Government

29

Consultant's view

1. Understanding of risk & impact concepts
2. Experienced in (all aspects of?) BCM
3. Outside agent independently advising Board regarding team composition
4. Plan writer (!)
5. Test manager
6. 2nd opinion
7. Pre-Auditor (end result or BCM process)
8. Soundboard for Board or management

30

Thank You!

31

More Info

- Jacques Heide
  ICTAS n.v.
  P.O.Box 491
  Curaçao, N.A.
  www.ICTAS.com
  jheide@ictas.com
  +599 9 513-3717

32