Business Continuity Management

A Supervisors perspective

24 June 2010, Curacao

Evert Koning, DNB

De Nederlandsche Bank
Eurosysteem

Agenda

- ***Introduction***
- BCM in reality
- Translation to Supervision

De Nederlandsche Bank
Eurosysteem

Biografy

- **Biography of Evert Koning:**
- Evert Koning is head of the department ICT Supervision within the Dutch Central Bank. This department of 16 people consists of CISA's with at least three to five years of relevant working experience. They support the other 14 inspection teams with interviews and investigations on the ICT topic.
- Evert himself joined Supervision within DNB in 1991 where he started with general supervision. After 6 years he focussed on ICT Supervision and as such he was one of the founding fathers of the Department he later headed. He started his career with the internal audit department of ABNAMRO Bank.
- **Education**: after a Masters in business economics he followed a post graduate in Accountancy (RA) and later in EDP-audit (RE) and finally he did the CISA exam.
- **International experience:** the membership of the Y2K Task Force of the Joint Forum. Later he was the founding father of the International ICT Supervision Conferences started in the end of 2002 in Amsterdam, the so called ITSG.
- **Contacts with ISACA**: Evert spoke on the Eurocacs 2002 in Budapest, 2008 Stockholm and was part of the programme committee of Eurocacs 2003 in Amsterdam. In 2003 he did a mediation assignment for the NL chapter with respect to Governance. Evert is also a frequent participant of the International Conference of ISACA.
- **Contacts with NOREA** (Dutch professional organisation): Board member (vice president) and former committee member

De Nederlandsche Bank
Eurosysteem

Origination ITSG

- Start during 2002
- Follow-up from Y2K Task Force
- Bilateral more time consuming
- No colleges of supervisors yet

De Nederlandsche Bank
Eurosysteem

Terms of reference

- The group provides an informal platform for intensifying international co-operation and information exchange on IT and specific IT risks between Heads of IT Supervision at Banking Regulators. The group will also provide an opportunity for greater knowledge of the different supervisory approaches, but will be mindful of local regulatory approaches and policies.
- The group is not a policy making forum, but is available to provide expert advice to international groups such as Basel and the Joint Forum.

De Nederlandsche Bank
Eurosysteem

Terms of reference

- **Objectives:**
- Exchanging information on technology risks and supervisory practices
- Establishing an international network for IT supervisors
- Promoting efficiency and synergy through cross-border supervisory work
- Facilitating sound practices in IT supervision
- Facilitating cross-border incident management
- **Membership**
- Membership of the group is heads (or representatives) of IT Supervisors examination departments within banking and governmental regulatory organisations.

De Nederlandsche Bank
Eurosysteem

Terms of reference

- **Activities**
- Annual conference for Heads of IT Supervision or representatives with a focused and technical knowledge of the IT environment within banking institutions, especially with respect to IT security and continuity.
- The conference will last several days with one or two representatives from each supervisory organisation. It is hosted on a rotational basis.
- The agenda of the conference should cover IT topics/risks which are collected in advance by the participants.
- The content of the conference encompasses round tables on relevant IT-topics, individual presentations on newly IT-developments, case studies, identification and sharing of common concerns and agreements on similar supervisory approaches in IT-examinations. Preparation and discussion papers send in advance will contribute positively to an efficient conference. At the end of the conference a draft for the next agenda can be developed. The host is responsible for aggregating the results of the conference and distributing these to the participants.

De Nederlandsche Bank
Eurosysteem

Terms of reference

- Consider opportunities for greater communication by e-mail / website / teleconferencing on supervisory issues and work
- Considering opportunities for providing collaborative training
- Considering opportunities for collaborative supervisory work

De Nederlandsche Bank
Eurosysteem

The conferences

- 2002 Amsterdam
- 2004 San Antonio
- 2005 London
- 2006 Hong Kong
- 2007 Toronto
- 2008 Rome
- 2009 Washington
- 2010 Sydney
- 2011 Mexico-city

De Nederlandsche Bank
Eurosysteem

Current core group

- Americas: FDIC, FRB, OCC, OTS, OSFI, CNBV
- Europe: CBFA, CSSF, BaFin, CB, FI, FT, FSA, BdI,
- BdS, DNB
- Asia: MAS, HKMA, CBRC, APRA, BoJ

De Nederlandsche Bank
Eurosysteem

New entrants

- **Guiding Principles for Admission of New Members:**
  - 1)Ensure that any process for bringing in new members does not negatively impact the character of ITSG and that ITSG still remains effective as an “informal and friendly” forum to discuss IT supervisory themes.
  - 2)The process is transparent, fair and not burdensome to administer.
  - 3)The current membership of ITSG (as of May 2009) is “confirmed” based on attendance at the earlier ITSG meetings. These countries (or supervisory agencies) will be automatically invited to all future ITSG meetings. This suggested approach for new membership will apply on a ‘go forward’ basis starting with new prospects interested in attending the upcoming ITSG meeting in Sydney (hosted by APRA).
  - 4)New members will be admitted to ITSG in a phased manner where country (or supervisory agency) will be initially invited to attend one or more ITSG meetings and then, subject to a broader ITSG decision, confirmed as a permanent/regular invitee to ITSG.
  - 5)The admission of new members as initial invitees will be based on specific criteria.

De Nederlandsche Bank
Eurosysteem

New entrants

- **New Membership Admission Criteria:**

- For initially inviting new attendees, requests should be conveyed to the relevant host country by a sponsoring permanent member. The request should address the criteria listed below. As the host country will play a key role as the sponsor of the specific ITSG session, it will have the responsibility of accepting or rejecting requests for non-permanent attendees to attend. The expectation is that current/confirmed members will be automatically invited but the new invitees will be subject to host country's assessment of its costs, the logistical arrangements for number/composition of the participants and consideration of these admission criteria.

De Nederlandsche Bank
Eurosysteem

New entrants

- The following criteria (membership and/or admission process-related) are proposed for admission of new members - initially as ‘invitees’ and also for consideration towards confirming their phased induction as confirmed permanent membership - for future ITSG meetings. It is suggested that any new member being considered meets one or more of the following -
  - 1)Represents a country/geographical region which enhances the diversity of the ITSG coverage, without over-representation of any one region to the detriment of other ITSG members/regions
  - 2)Represents a significant population base of large/international financial institutions either in its own domestic market or as an offshore financial services centre; or as a major IT services industry supporting the international financial sector.

De Nederlandsche Bank
Eurosysteem

New entrants

- 3)Can potentially add value to ITSG in terms of its supervisory profile, size and/or skills-base.
- 4)Is willing and able to contribute to ITSG either as a presenter, active group member for a specific IT supervisory theme and/or potentially as a host of an ITSG session.
- 5)Is willing to adapt to and work within the informal setting of the ITSG.
- 6)Offers some unique value proposition to ITSG, not mentioned above.
- 7)Is willing (if requested by host country) to send some background information email or communication to indicate how the prospective member meets one or more of these criteria.

De Nederlandsche Bank
Eurosysteem

New entrants

- It is suggested that initial invitations to new members for their first ITSG do not automatically guarantee confirmation to future ITSG meetings. As a proposal, they would need to be invited to 2 ITSG meetings after which, based on the general review of the attendees' participation and contribution at the ITSG their confirmation can be proposed by the inviting host and supported by a simple majority of participating countries.

De Nederlandsche Bank
Eurosysteem

Sub groups

- Links by regional contacts
- European meeting
- FFIEC: IT subcomittee
- Topics working groups

De Nederlandsche Bank
Eurosysteem

Some important topics

- Peer reviews
- BCM/Pandemic
- Security/Cybercrime
- Outsourcing/Offshoring

De Nederlandsche Bank
Eurosysteem

Agenda

- Introduction
- ***BCM in reality***
- Translation to Supervision

De Nederlandsche Bank
Eurosysteem

Business could be disrupted anytime, anywhere

De Nederlandsche Bank
Eurosysteem

BCM is important

- Disaster is defined as “any unplanned & unforeseen event, which makes the facility (or system) inoperable or inaccessible”.
  - 20% of companies suffer a major disaster every 5 years
  - 90% of companies have had at least one serious security breach in the last two years
  - 70% of companies suffer systems downtime at least once a year
- Of companies without adequate business continuity plans:
  - 40% fail within 18 months
  - 12% fail within 5 years
  - 40% never reopen
  - 8% survive

Source: Guardian IT

De Nederlandsche Bank
Eurosysteem

International standards for BCM

- **BS25999** – Business Continuity Management Standard (1) Code of Practice, (2) Specification for Business Continuity Management
- **ISO/IEC 24762** – Guidelines for information and communications technology disaster recovery services
- **ISO/PAS 22399** - Societal security - Guideline for incident preparedness and operational continuity management
- **ISO/IEC 27002** - Security techniques - Code of practice for information security management

ISO

BSI
British Standards

De Nederlandsche Bank
Eurosysteem

BCM Defined

…the development of strategies, plans and actions which provide protection or alternative modes of operation for those activities or business processes which, if they were to be interrupted, might otherwise bring about a seriously damaging or potentially fatal loss to the enterprise.

Source: BS25999

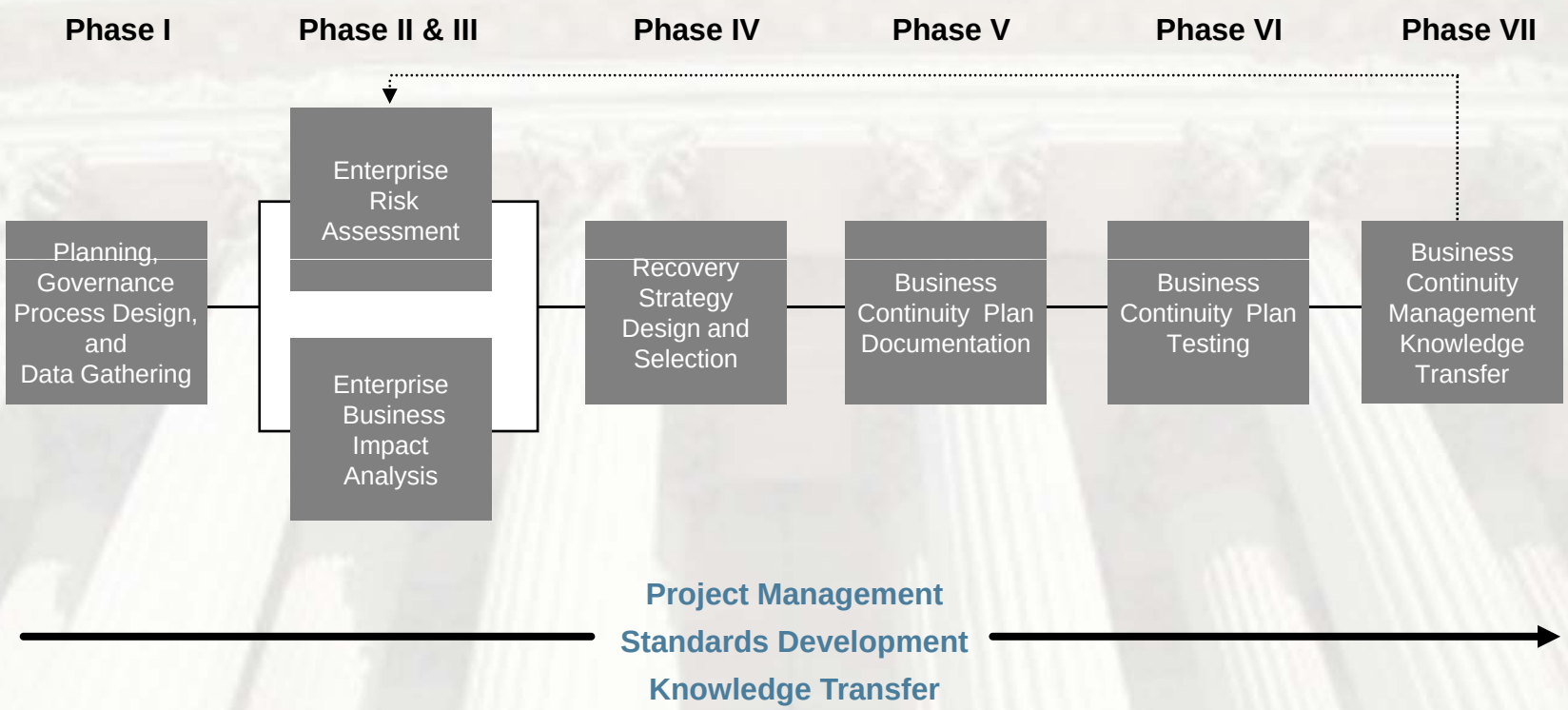
A whole of business approach that includes policies, standards, and procedures for ensuring that specified operations can be maintained or recovered in a timely fashion in the event of a disruption. Its purpose is to minimise the operational, financial, legal, reputational and other material consequences arising from a disruption.

Source: Basel II – High level principles for business continuity

BCM = Crisis Management + Business Continuity Planning + IT Disaster Recovery Planning

De Nederlandsche Bank
Eurosysteem

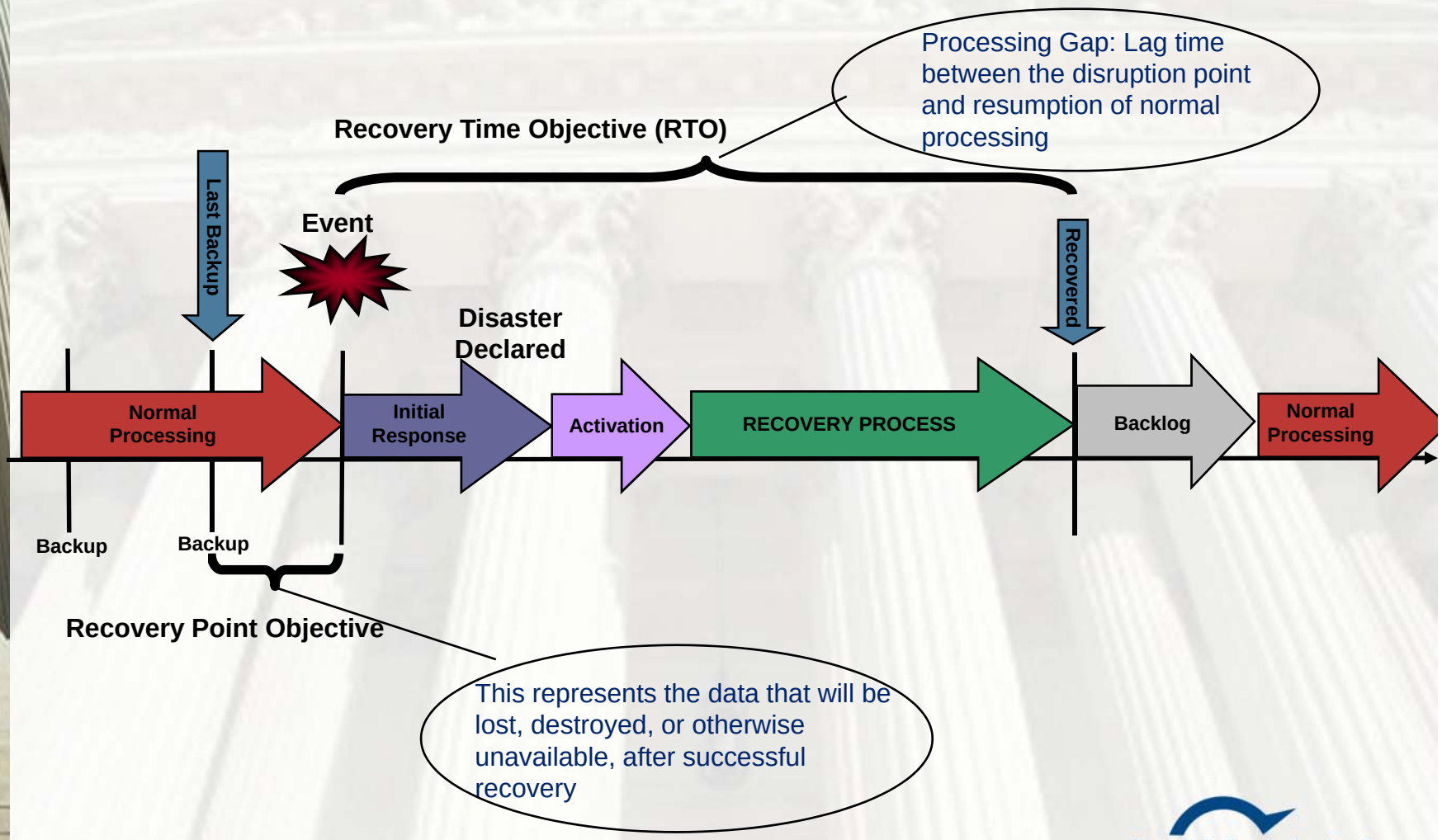
Effective BCM



Based on BS25999 – High level principles for business continuity

De Nederlandsche Bank
Eurosysteem

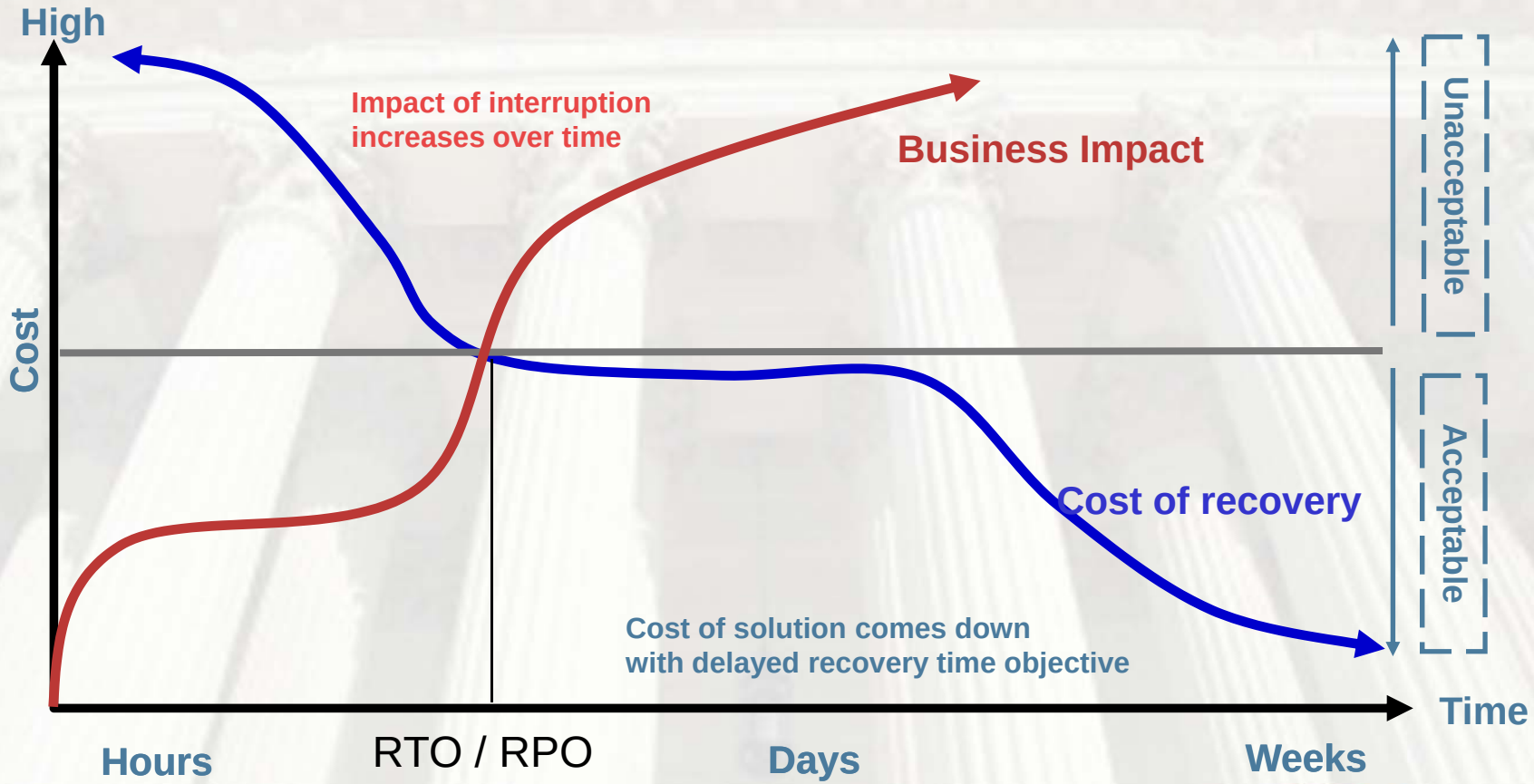
Business Impact Analysis (I)



De Nederlandsche Bank
Eurosysteem

Business Impact Analysis (II)

The goal is to determine the optimum investment related to discountinuity.



BCP - 10 Common problems (I)

1. Not understanding the difference between Risk and Impact, when impact is the area that should be focused upon.
2. Composition of the Recovery Team. Often the team for political reasons contained too many senior executives, who were strategic thinkers rather than operational people. Meanwhile, team deputies were too often not trained.
3. No plan maintenance. Plans were often just “shelfware” – they sat on a shelf after being written.
4. Poorly defined roles and responsibilities. They were often undefined, too generic, or too specific to an individual.
5. Inadequate objectives, too much focused on technological rather than business goals.
6. No time management element. Plans need critical milestones for the 48 hours after an incident, to allow problems to be identified and dealt with more quickly.

Source: Allen Johnson of consulting firm Scenaris

BCP 10 Common problems (II)

7. No checklists. Too often business continuity plans consisted of long prose rather than simple checklists. Checklists were necessary for everyone, but particularly so in cross-border organisations using multiple languages.
8. Too much complexity in plans, often involving incorrect or out-of-date details.
9. Weak strategies. One example was reciprocal arrangements for firms to share each others' office space in the event of a disaster. These were unworkable and were not even legally binding unless a payment changed hands.
10. No conducting of exercises or tests. Firms might avoid conducting a test so as not to have it fail. To overcome this obstacle, initial exercises should not be too complex and should not be based on too extreme a scenario. Meanwhile it was also important that exercises involving senior management were designed with genuine learning goals in mind rather than simply to provide an exciting experience.

Source: Allen Johnson of consulting firm Scenaris

Continuity Risk Finance Industry

Some characteristics:

- International and sometimes national guidance (f.e. Basel II – High level principles for business continuity and Toetsingskader BCP Financiele Kerninfrastructuur)
- Interdependency of financial institutions and markets
- Some institutions are critical for the financial system
- Law of big numbers
- Chain effect: impact on the real economy, other industries and worldwide.

De Nederlandsche Bank
Eurosysteem

Agenda

- Introduction
- BCM in reality
- ***Translation to Supervision***

De Nederlandsche Bank
Eurosysteem

How DNB deals with Continuity Risk

- Established consensus with financial industry participants about acceptable standards for business continuity.
- In case the financial system could be or is really frustrated, DNB will coordinate such crisis and will initiate the emergency plans.
- A core element of DNB's supervision activities including periodic follow-up.
- Taking part of a yearly payment system connectivity check.
- International, DNB shares experiences in reviewing and enhancing BCP's.
- Depending on certain threats, DNB performs specific actions. For instance, in case of pandemic flew.

De Nederlandsche Bank
Eurosysteem

FIRM

- Business continuity and
- Also one of four IT risk categories

Continuity

  – Risk of continuity of the most important business processes of the institution due to failure, disability of the IT infrastructure (both applications and systems)

De Nederlandsche Bank
Eurosysteem

Supervisors expectations

- General points
- Smaller institutions
- Bigger institutions

De Nederlandsche Bank
Eurosysteem

General Points

- BCM Proces
- BIA and risk analysis (scenarios)
- Data classification, critical processes, spof
- BCP, control measures, risk mitigation
- Policies and procedures
- Testing and training
- Communication, crisismanagement

De Nederlandsche Bank
Eurosysteem

Smaller Institutions

- Escrow agreement
- Back-up stored external (data and software)
- Yearly tests
- Contract for hardware
- Dataclassification

De Nederlandsche Bank
Eurosysteem

Bigger institutions

- Hot stand-by
- Own contingent site
- Mirroring

De Nederlandsche Bank
Eurosysteem

ITSG agreement on disaster recovery testing

During the European ITSG conference in 2009 and the recent one in March 2010 Australia, it was agreed that a yearly complete disaster recovery test (by putting the plug out) of datacenters won't be required by regulators.

The related risk, especially for the system banks, is considered to be too high.

Escalation Committee on Payments and Securities

- Mandate: To solve acute problems in a crisis in payments and securities
- Members: 10 biggest banks, Equence, Netherlands bankers' Association, Euronext, LCH, Clearnet, Euroclear and DNB
- Chair and Secretariat at DNB
- Delegates have the authority for binding decisions on behalf of their institution
- Responsible for good communication

National guidance on BCM

1. Every institution has a Business Continuity Plan approved by its Executive Board
2. Risk analyses of critical systems and businesses
3. Explicit attention to human factor
4. An internal crisis organisation
5. What are the single points of failure
6. A secondary site
7. Critical processes and systems must be restored as soon as possible
8. Testing of systems and business
9. Communication plan for all stakeholders

The Dutch core financial system has to apply to the above guidance, which is part of the so called ‘Red Book’ (so called Toetsingskader BCP Financiele Kerninfrastructuur)

De Nederlandsche Bank
Eurosysteem

Yearly BCM assessment

BCM within the Dutch banking industry, being part of the vital infrastructure, is yearly assessed. Focus could be the retail, wholesale or securitisation function depending on level of criticality.

De Nederlandsche Bank
Eurosysteem

Investigation - Approach

- A framework of 5 areas was made for the investigation :
  1. Strategy and policy
  2. Organisation and design
  3. Business Continuity and Disaster Recovery Plans
  4. Testing
  5. Quality assurance
- Scores defined
- A report lay-out was defined

De Nederlandsche Bank
Eurosysteem

Investigation - Results

- Bottlenecks more in tuning measures of IT and business
- Results were reported to the institutions, including relative position to other banks
- Decision with respect to follow-up
- Future focus on service providers
- Update “toetsingskader”
- Experiences of sector wide testing

Resources for Research

- Disaster Recovery Institute International www.drii.org
- Global Continuity www.globalcontinuity.com
- Federal Emergency Management Agency www.fema.gov
- Association of Contingency Planners www.acp-international.com
- Bank for International Settlements www.bis.org
- British Standard Institute www.bsigroup.com
- International Organization for Standardization www.iso.org

De Nederlandsche Bank
Eurosysteem

e.koning@dnb.nl

De Nederlandsche Bank
Eurosysteem