Title: ABN AMRO bank remarks on "Principles for Financial market infrastructures".
Author: E. Smit MBCI ABN AMRO TOPS/ BRO/ BCM
Email: Egbert.Smit@nl.ABNAMRO.com

General:
The principles in general and Principle 17 in particular does not single out 'business continuity management' as a discipline in its own right. I suggest having an explicit mentioning of BCM as part of this principle instead of BCM for separate elements of the Principles.

Within the Dutch financial sector parties have worked together to define general BCM principles (independent from specific standards such as the primarily UK based BS25999), see the included "Proposed principles for BCM requirements for the Dutch financial sector and its providers."

A sound description of BCM is missing. In several principles parts of BCM are mentioned as stand alone solutions in stead of the managed approach and implementation BCM should be.

Principle 17 (page 75):
Page 75 - Minimise their impact should be: mitigate to a regulatory stated level or if not defined to a predefined and by the responsible management accepted level.
Page 76 point 5 - critical information technology (IT) systems: which systems are mend? I suppose that this not applies to ALL critical systems within the FMI.
Page 77 3.17.7 - …to minimise operational risk: should be mitigate to a regulatory stated level or if not defined to a predefined and by the responsible management accepted level.
Page 79/79 3.17.11 - …should have well-defined policies …..: if BCM is correctly defined (see principles for BCM requirements) this is already taken care of.
Page 79 3.17.2 - Business continuity planning: this is to simplistic, it's better to speak about Business Continuity Management.
Page 79 3.17.13 - The secondary site should provide levels…..: This should be: The secondary site should provide levels of service **of the critical services** similar to those….
Page 79 3.17.13 - ….third site…: unnecessary rule, the FMI should be held to its responsibilities; it is up to the FMI how it wants to implement this.

Proposed principles for BCM requirements for the Dutch Financial sector and its providers.

BC-VIF Werkgroep BCM requirements

March 24th , 2011

Owner	Business Continuity – Vital Infrastruture Finance - ‘projectgroup BCM requirements’
Authors	Carol Meeuwisse (Equens) Fred van Benschop (Rabobank) Ruud Goudriaan (ING) Ted Smets (SNS-bank) Egbert Smit (ABN AMRO) (chairman)
Version	2.0 (March 24th 2011)
Status	Final
Endorsed by	ABN AMRO, BNG, DNB, Equens, LCH Clearnet, Euroclear NL, ING, NVB, NYSE Euronext, RABObank, RBS, SNS Reaal, SNS, SWIFT.
Security	Internal only, Confidential

Table of Contents

1 Introduction

This document is intended to formulate sector wide accepted and suitable principles for Business Continuity Management (BCM) requirements implementation. These principles are formulated because there is not a commonly used and accepted, worldwide, BCM standard.

These principles are meant for all financial institutions, financial markets infrastructures (fmi) and external (third party) vendors in the Financial sector who support the financial institutes critical business processes.

With the implementation of these principles throughout the Financial sector, every organisation within the Financial sector can be on the same level of BCM maturity. This is not only beneficial for each individual organisation but also for the Financial sector as a whole. The principles facilitate the management of Service Level Agreements in general.

These principles should therefore be used by independent (external) parties as well as internal audit departments to get an unambiguous (sector wide comparable) view of the status of the BCM implementation within the organisation and subsequently of the Financial sector.

2 Policy

2.1 Introduction

Every organisation shall have a BCM policy. This BCM policy describes the starting points and parameters for the business continuity implementation.

2.2 Objective

The organisation shall develop its Business Continuity policy which states the objectives of BCM within the organisation. Initially, this may be a high level statement of intent which is refined and enhanced as the capability is developed.
The Business Continuity policy shall provide the organisation with documented principles to which it will aspire and against which its Business Continuity capability should be measured.

2.3 Requirement

The organisation is able to prove that the objective is implemented, maintained, periodically assessed and/or reviewed and provides adequate assurance (in line with the organisation's, its stakeholders and customers needs) for the organisation. The BCM policy shall be owned at a high level, e.g. a board director or elected representative.

The scope of the BCM policy clearly defines the legal and other obligations and any limitations or exclusions that apply, e.g. geographical or otherwise.

Product for chapter 2: Policy document including principles accepted and signed off by the senior management accountable.

Preferred implementation (should contain at least):

- *define the scope of BCM within the organization;*
- *BCM resourcing with clear responsibilities and accountabilities (RACI);*
- *define the BCM principles, guidelines and minimum standards for the organization such as (but not limited to):*
  - *scope (geographic, organizational, etc.);*
  - *risk appetite;*
  - *risk mitigation policies;*
  - *impact categories and qualitative or quantitative rating descriptors;*
  - *regulatory requirements;*
- *refer to relevant standards, regulations or policies that have to be included or can be used as a benchmark.*

3 Business Continuity Governance

3.1 Introduction

BCM management and governance are at the heart of the BCM process. Effective governance establishes the organisation's approach to Business Continuity.
The participation of top management is key to ensure that the BCM process is correctly introduced, adequately supported and established as part of the organisation's culture.

3.2 Objective

3.2.1 General

Create, implement and maintain an adequate Business Continuity governance structure.

3.2.2 Monitoring and Reviewing

To ensure that management monitor and review the effectiveness and efficiency of Business Continuity Management, review the appropriateness of the implementation of the Continuity Risk policy, objectives and scope and determine and authorise actions for remediation and improvement.

3.2.3 Maintenance and Improvement

To maintain and improve the effectiveness and efficiency of the Business Continuity Management implementation by taking preventive and corrective actions as determined by the management review.

3.3 Requirement

3.3.1 General

The organisation should be able to prove that the objective is implemented, maintained, periodically assessed, and tested or audited to supply adequate assurance (in line with the organisations BCM policy) for the organisation.

3.3.2 Monitoring and Reviewing

(BC)Management shall review the organisation's Business Continuity Management implementation at planned periodic intervals and / or when significant changes occur to ensure its continuing suitability, adequacy and effectiveness.

3.3.3 Maintenance and Improvement

The organisation shall continually improve the effectiveness of the Business Continuity Management System.

Product for chapter 3**:** Periodic review report including improvement actions (when applicable).

4 Business Impact Analyses

4.1 Introduction

The understanding of the organisation through the identification of its key value chains, processes, products and services and the critical activities and resources that support them is essential to align BCM to the business goals. The process to identify and document this is commonly referred to as the Business Impact Analysis (BIA).

4.2 Objective

The objective of the Business Impact Analysis is to identify all critical value chains, processes and resources by determining the impact of a disruption in terms of Maximum Tolerable Period of Disruption (MTPD) on all the business value chains, processes and resources and to determine the minimum requirements (statutory, regulatory, contractual, commercial) necessary for resumption of the identified critical value chains, processes and resources. The BIA usually establishes an impact associated with the disruption lasting varying lengths of time. Impact estimates may include actual financial impacts and non-financial impacts (such as regulatory and reputational impact).

4.3 Requirement

The BIA should assess all business activities and resources.

Product for chapter 4: Overview of all critical value chains, processes and resources including the MTPD.

Preferred implementation (should contain at least)*:*

- *Identification of the critical business activities and resources. The public role of financial institutes should be taken into consideration in this process. The use of a structured and applicable classification model to support this process is recommended.*
- *The Maximum Tolerable Period of Disruption (MTPD) – or maximum downtime or maximum outage time -, the duration after which an organization's viability will be irrevocably threatened if product and services delivery cannot be resumed.*
- *The Recovery Time Objective (RTO), the target time set for resumption of the business process or activity after an incident.*
- *The Recovery Point Objective (RPO), the point in time from where the critical data for the business process or activity must be restored after an incident.*
- *The minimum requirements necessary for executing the business process in terms of:*
  - *Number of employees and, if applicable, named staff (SPOC's);*
  - *Number of desks and facilities (i.e. PC's, Telephone's, Printers, Scanners etc.);*
  - *Information Systems and Applications, including necessary data;*
  - *Minimal services levels to (internal) customers;*
  - *Dependency of third party suppliers (internal or external*).

5 Risk Assessment/Analysis

5.1 Introduction

The outcome of the Business Impact Analysis enables the organisation to focus its risk assessment (RA) on the (Mission) critical activities of the organisation rather than conducting a traditional all risks analysis.
Definition Risk assessment: overall process of risk identification, analysis and evaluation.

5.2 Objective

The objective of a risk assessment is to identify the internal and external threats, liabilities and exposure, including risk concentrations that could cause the disruption, interruption or loss to an organisation's mission critical activities. Threats can be assessed using risk scenario's or Basel event types.

5.3 Requirement

A Risk analysis including the accepted levels of risk, mitigating actions (if applicable) and accepted residual risks.

Product for chapter 5: A risk assessment and analysis report.

Preferred implementation (should contain at least)*:*

- *The scope of the research including the areas of risk (minimal research risk areas are: Human factor, assets, and facilities.*
- *The criteria for evaluation of risk (4T-model = take, treat, transfer, terminate).*
- *The vulnerability and exposure (likelihood of occurrence) of the organisation to specific types of threat.*
- *Risk concentration(s) e.g. where a number of Mission Critical Activities are located within the same building or on the same site.*
- *A risk assessment and analysis (combined with a Business Impact Analysis) to inform and enable the setting of a risk appetite.*
- *A prioritised focus of BCM and risk controls.*
- *A risk control management strategy and action plan*.
- *The likelihood (probability or frequency) of a threat occurring.*
- *How vulnerable an organisation is to the various types of threat and enables their prioritisation and control management.*
- *A basis to establish a risk appetite and risk management control programme and action plan.*

6 Business Continuity Strategy

6.1 Introduction

A good strategy analysis is an important precondition for the choice (and/or combination) of cost-effective continuity measures. The strategy must match the value of objects and the outcome of the business impact and risk analysis. Alternative strategies are investigated on cost-effectiveness. In the analysis of alternative continuity strategies business solutions and technical solutions should be reviewed in conjunction.

Continuity strategies can be divided into control strategies and recovery strategies. The control strategies describe what measures the organisation owns to control risks and how they are applied. Recovery strategies describe what measures the institution has to return to a normal situation from a calamity and how they are applied.

6.2 Objective

Define risk reducing and recovery strategies to limit the probability of occurrence and/or the impact of disasters.

6.3 Requirement

Adequately defined (in accordance with the BCM policy) risk reducing and recovery strategies including necessary measures.

Product for chapter 6: BCM strategy document.

Preferred implementation (should contain at least):

- *All key requirements matching the value of objects and BIA and RA results;*
- *chosen prevention strategies;*
- *chosen recovery strategies;*
- *chosen control strategies;*
- *Residual risks strategy.*

7 *Business Continuity Plan*

7.1 Introduction

Every organisation is in risk from potential disasters that may lead to loss of staff, public as well as private infrastructure, buildings, critical business processes, ICT infrastructure, data (electronic and physical) and communication. Creating and maintaining a Business Continuity Plan helps to ensure that the organisation has the information and resources to deal with those disasters.

7.2 Objective

A Business Continuity Plan is a set of procedures and information, designed to help ensure recovery from the effects of the various threat scenarios. It addresses the recovery steps from the time of disruption, until the time all critical services and supporting operational functions are recovered to an acceptable, predefined level

7.3 Requirement

A plan describing a necessary measures to enable the restart of the disturbed key values chains, processes and/or products.

Product for chapter 7: Business Continuity Plan. The BCP can also be a compound of partial BCP's.

Preferred implementation (should contain at least)*:*

- *Contain a description of its scope;*
- *Have an owner;*
- *Be reviewed periodically;*
- *Describe the BCM recovery procedures, such as, but not limited:*
  - *Informing and alerting;*
  - *Description of first and immediate actions;*
  - *Mobilisation;*
  - *Response, including risk scenario's;*
  - *Escalation and up scaling;*
  - *Downscaling;*
  - *Evaluation and reporting;*
- *Contain relevant information about at least:*
  - *the outcome of the business impact analysis, risk assessment and continuity strategy processes;*
  - *the crisis management organisation, including roles, authorities and responsibilities, (alternative) locations and procedures that deal with information, decision making and action following;*
  - *crisis communication, including call procedures and call trees, communication strategy to all stakeholders, media interfaces and spokespeople*.

8 Exercise BCM arrangements

8.1 Introduction

The BCM plans (Business Continuity, Disaster Recovery and Crisis Management) cannot be considered robust and reliable until exercised. The purpose of any exercise and subsequent evaluation is to determine the feasibility of the plans, identify deficiencies, improve the plans, provide a mechanism for maintaining and updating the plan, meet regulatory requirements and is not to assess personal performance. The risk associated with exercising shall be understood. The exercise shall not expose the organisation to an unacceptable level of risk.

8.2 Objective

The objective of exercising BCM arrangements is to ensure that the continuity arrangements (BC, DR and CM) are validated by exercise and review and are kept up to date. Exercising also raises the competence of the crisis management organisation.

8.3 Requirement

All Business Continuity Plans, Disaster Recovery Plans and Crisis Management Plans for critical value chains, business functions, products or activities shall be maintained and tested periodically according to the defined exercise and test levels.

Product for chapter 8: BCM test and exercise plan including observed gaps, issues and corrective measures.

Preferred implementation (should contain at least):

- *Exercising*
  - *The BCM vendor shall exercise its Continuity arrangements to ensure that they meet business continuity requirements.*
- *Managing the Exercise*
  - *A clear exercise command structure shall be applied with roles and responsibilities allocated to appropriate individuals.*
- *Planning exercises*
  - *Exercises shall be realistic, carefully planned and agreed with stakeholders, so that there is minimum risk of disruption to business processes. They shall not, however, be carried out during incidents.*
- *Exercise and Test levels*
  - *In most instances, the whole set of business continuity, disaster recovery or crisis management exercises cannot be executed in one exercise. A progressive exercising regime is therefore appropriate to build towards a full simulation of a real incident. Exercises shall be progressive to include an increasing test of dependencies and inter-relationships and relevant end-user communities.*
- *Sign-off*
  - *Business Continuity Plans, Disaster Recovery Plans and Crisis Management Plans, and the successful execution of tests and exercises shall be signed off by senior management.*

9 Crisis Management

9.1 Introduction

Crisis Management is the process by which an organisation deals with a major event that threatens to harm the organisation, its stakeholders, the financial sector or the general public. Key elements of a crisis and Crisis Management are (a) a threat to the organisation or the financial sector, (b) the element of surprise, (c) a short decision time.

9.2 Objective

The organisation should install and maintain an adequate Crisis Management structure consisting of at least a:
- Crisis Management Team;
- Crisis Management Plan.

9.3 Requirement

The organisation should be able to prove that the objective is implemented, maintained, periodically assessed and/ or tested and adequate (in line with the organisations BCM policy) for the organisation.

Product for chapter 9: Periodic Crisis Management Organisation review report including improvement actions (if applicable).

Preferred implementation (should contain at least):

- *Date of last review;*
- *Date of last test;*
- *Date of last audit;*
- *Test plan;*
- *Observed gaps/omissions/issues (including an owner);*
- *Due dates for solving the gaps/omissions/issues.*