Principles for BCM requirements for the Dutch financial sector and its providers.

Platform Business Continuity Vitale Infrastructuur Financiële sector (BC VIF)
Werkgroep BCM requirements
21 September 2011

Version 2.0

Owner	Platform BC-VIF
Authors	Working group BCM requirements
Version	1.0 (21 September 2011)
Status	Final
Members	ABN AMRO, ABN AMRO Clearing Bank, Currence, DNB, EMCF, Equens, Euroclear Nederland, ING, KAS BANK, LCH.Clearnet SA, Ministerie van Financiën, NVB, NYSE Euronext, Rabobank, RBS, SNS Bank, SWIFT.
Security	Public

Table of Contents

1 Introduction

This document is composed by the 'platform Business Continuity Vitale Infrastructuur Financiële sector (BC VIF) and intended to formulate sector-wide accepted and suitable principles for Business Continuity Management (BCM) requirements. These principles are provided because there is no commonly used and accepted, worldwide BCM standard for financial institutions.

These principles are meant for all financial institutions, Financial Markets Infrastructures (FMIs) and external (third party) providers in the financial sector who support the financial institutions' critical business processes.

The principles in this document harmonise and, where appropriate, strengthen the existing national and international standards on BCM and provide a commonly used and acceptable framework for financial institutions. As a main reference and source of information the following standards and practises are used:
- British Continuity Institute – Good Practise Guidelines (GPG);
- British Standards Institute – BS25999 part 1 and 2;
- US Disaster Recovery Institute – Generally Accepted Practises (GAP);
- US National Fire Protection Association – NFPA1600.

The principles are a minimum set of BCM requirements and are written without the intent to specify specific solutions or implementation rules. The principles are defined at a level as high as possible to enable organisations to take their responsibilities and endorse and implement the principles. This is not only beneficial for each individual organisation but also for the financial sector as a whole.

The principles provide a common framework that supports the definition of specific assessment frameworks for financial institutions and provider groups such as IT and telecom service providers and vendors. The principles also provide a framework for BCM requirements to be taken into account in Service Level Agreements (SLAs) in general.

In this document the term "principles" is used as a generic term to cover all normative statements such as standards, principles, recommendations and responsibilities.

2 Policy (Principle 1)

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 BCM 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 BCM policy provides 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 BCM policy is implemented, maintained, periodically assessed and/or reviewed. 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 Principle 1: BCM 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 organisation such as (but not limited to):*
  - *Scope (geographic, organisational, 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 (Principle 2)

3.1 Introduction

Business continuity 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 crucial to ensure that the BCM process is correctly introduced, adequately supported and established as part of the organisation's culture.

3.2 Objective

Establish, implement and maintain an adequate business continuity governance structure to ensure that management monitors, reviews, maintains and improves the effectiveness and efficiency of the BCM implementation.

3.3 Requirement

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

Management shall review the appropriateness of the implementation of the BCM policy, objectives and scope, and determine and authorise actions for remediation and improvement at planned periodic intervals and/or when significant changes occur to ensure its continuing suitability, adequacy and effectiveness.

The organisation shall continually improve the effectiveness of BCM by taking preventive and corrective actions as determined by the management review.

Product for Principle 2**:** Periodic review report including improvement actions (when applicable).

4 Business impact analysis (Principle 3)

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 of identifying and documenting is commonly referred to as the Business Impact Analysis (BIA).

4.2 Objective

The objective of the BIA 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 Principle 3: 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 organisation'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 (SPOCs);*
  - *Number of desks and facilities, i.e. PCs, telephones, 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 (Principle 4)

5.1 Introduction

The outcome of the BIA 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 of risk assessment: overall process of risk identification, analysis and evaluation.

5.2 Objective

The objective of an RA 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 scenarios or Basel event types. The risk analysis must concern itself explicitly with the organisation's dependence on utilities and basic facilities (power, gas, water, telecommunications) and external service providers; the specific risks that such dependence implies for the continuity of critical processes and the measures taken against each such risk to ensure continuity.

5.3 Requirement

An RA including the accepted levels of risk, mitigating actions (if applicable) and accepted residual risks.

Product for Principle 4: 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 (Principle 5)

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, 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 Principle 5: BC strategy document.

Preferred implementation (should contain at least):

- *All key requirements matching the value of objects and BIA and RA results.*
- *Prevention strategies.*
- *Recovery strategies.*
- *Control strategies.*
- *Residual risks strategy.*

7 *Business continuity plan (Principle 6)*

7.1 Introduction

Every organisation is in risk from potential disasters that might 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 (BCP) helps to ensure that the organisation has the information and resources to deal with those disasters.

7.2 Objective

A BCP 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 the disruption, until the time that all critical services and supporting operational functions are recovered to an acceptable, predefined level. The BCP must specify clearly what agreements have been made with the service providers, the form and manner in which information on the measures of the service providers and their performance in relation to the service level agreements is available, and how guarantees are obtained with respect to implementation and operation of these measures.

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 Principle 6: Business Continuity Plan (BCP). The BCP can also be a set of BCPs.

Preferred implementation (should contain at least)*:*

- *A description of its scope.*
- *Have an owner.*
- *Be reviewed periodically.*
- *Describe the BCM recovery procedures, such as, but not limited to:*
  - *Informing and alerting;*
  - *Description of first and immediate actions;*
  - *Mobilisation;*
  - *Response, including risk scenarios;*
  - *Escalation and up scaling;*
  - *Downscaling;*
  - *Evaluation and reporting;*
- *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 (Principle 7)

8.1 Introduction

The BCM plans (Business Ccontinuity (BC), Disaster Recovery (DR) and Crisis Management (CM)) cannot be considered robust and reliable until exercised. The purpose of any exercise and subsequent evaluation is to determine the adequacy 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 improves the competence of the crisis management organisation.

8.3 Requirement

All BC, DR and CR 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 Principle 7: BCM test and exercise plan including observed gaps, issues and corrective measures.

Preferred implementation (should contain at least):

- *Exercising:*
  - *The organisation and the BCM providers (internal and external) 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 a 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*
  - *BC, DR and CR plans, and the successful execution of tests and exercises shall be signed off by senior management.*

9 Crisis management (Principle 8)

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 Principle 8: Periodic crisis management organisation review report including improvement actions (if applicable).

Preferred implementation (should contain at least):
- *Date of last review*
- *Date of last tes.t*
- *Date of last audit.*
- *Test plan.*
- *Observed gaps/omissions/issues (including an owner).*
- *Due dates for solving the gaps/omissions/issues.*

10 Definitions

Business continuity

The strategic and tactical capability to plan and prepare for and respond to disruptions and major incidents in order to continue operations at an acceptable predefined level.

Business continuity risk management

The process that identifies potential threats to the organisation and the impacts to the continuity of business operations that those threats, if realised, might cause. It provides a framework for building and maintaining organisational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities.

Crisis management

The process of preparing and responding to an unpredictable event or incident to prevent it from escalating into an even bigger problem, or worse, into a disaster. It also involves the execution of well-coordinated actions to control or resolve the damage and preserve or restore client confidence.

Disaster recovery

The process of restoring operations critical to the resumption of business, including regaining access to data (records, hardware, software, etc.), communications (incoming, outgoing, toll-free, fax, etc.), facilities, workspace, and other business processes after a disaster

Incident

For the purpose of continuity risk, the definition of an incident is an event that has the capacity to lead to loss of, or a disruption to, the organisation's operations, services or functions which if not managed can escalate into an emergency, crisis or disaster.