De Nederlandsche Bank N.V.

Payment Policy Division

1 January 2007

Assessment Framework
Business Continuity Planning (BCP)
Financial Core Infrastructure

Version: 2007

ASSESSMENT FRAMEWORK BCP FINANCIAL CORE INFRASTRUCTURE

In 2004 a business continuity planning (BCP) assessment framework has been drawn up on an interbank basis which banks, Equens, stock exchange institutions, other market participants and De Nederlandsche Bank (DNB) will use to amplify and update their BCP plans. In 2006 a review of this framework was performed. This review was part of the supervisory and oversight activities of DNB. The main changes are the replacement of standard 10 by appointments made with the financial sector and adding a guidance note regarding the implementation of the continuity of the human factor for critical systems/business processes.

The following nine BCP standards are proposed in order to serve as a general assessment framework for institutions belonging to the financial core infrastructure in the Netherlands. The standards are derived from international practices (including IMF practices). It is not the intention in advance that all the standards should be accorded similar weight and importance. In the case of the assessment framework, a distinction can be made between BCP activities which the institutions wish to impose on themselves and activities which DNB regards as a minimum for the institutions concerned.

1. Each institution must have a business continuity plan approved by the management board or senior management, which defines the strategy, business continuity objectives and critical operating processes and describes adequate continuity measures. Naturally, the security and protection of the staff takes precedence. The plan should be updated at least annually and more often if far-reaching changes are made to the organisation, operating processes or systems. The plan should specify the maximum acceptable time during which operating processes and systems are unable to function. It should also deal with the international dimension of the organisation and the consequences of, for example, outsourcing. It is advisable to consider having the BCP plan assessed by the internal audit department. Annex 2 contains an indicative list of relevant subjects that should be elaborated in a business continuity plan.

2. Each institution should have made a risk analysis of possible catastrophic events and, above all, their impact on essential systems and processes. In this connection, catastrophic event scenarios can be classified in the following categories: technical and organisational failure, deliberate human acts (terrorism, physical violence and cyber attacks) and natural disasters. This approach is in keeping with the current government projects on vital infrastructures and crisis management. In addition, acceptable residual risks should be indicated.

3. The business continuity plans should be transparent, in that they should show what measures have been taken to minimise the potential problem created by the human factor in the continuation of the operating processes and how the deployment of (other) staff can be organised after a catastrophic event. This applies both to the ICT and the business. It involves, in particular, an obligation on the part of the organisation to use its best endeavours, since this is a difficult condition to fulfil. Many of the institutions are considering the idea that part of the staff should always be off site (e.g. free). Annex 1 contains guidance for the possibilities of the implementation of the human factor.

4. Each institution should have a crisis organisation in order to be able to act in the event of an emergency. The crisis organisation should be controlled by the management board or senior management.

5. Each institution should make an analysis of the extent to which it is dependent on basic facilities (electricity, telecom, etc.) and external providers and how the back-up for them is organised. Single points of failure should be identified. This may be an organisational unit or the fact that only a single employee or a few employees have essential knowledge. Consideration should also be given to possible alternatives in order to safeguard the continuity of key facilities.

6. The essential operating processes and systems should be resumed as quickly as possible[1]. In this connection, a longer recovery period can apply to participants outside the core infrastructure.

7. Each institution should be able to switch its essential systems to a different centre which is at a sufficient distance from the primary site. What constitutes a sufficient distance depends on the risk profile. A time horizon for the expected outage or repair time should be adopted in this connection. In addition, there should be an assessment of the risks that are run in the case of a move to a back-up facility and in what circumstances these risks can be limited by repairing and restarting the system at the primary site.

8. Alternate systems and continuity and contingency procedures should be regularly tested. This involves testing of both the ICT systems and the staff (e.g. moving the business to a back-up site). Depending on the importance of the system and the business, this should be done at least once a year. If desired, agreements can be made for organising end-to-end testing of the entire chain (internally and externally). In addition, tests can be conducted of moves from primary site to secondary site and from secondary site to secondary site (however, this requires broad coordination within the core infrastructure).

9. Each institution should have a communication plan setting out how the communication to all stakeholders can be organised as effectively as possible in the event of a catastrophe (including the preparation of contact lists and messages).

[1] A repair or back-up period of four hours could apply to the financial core infrastructure, including decision-making and traveling time. In due course this could be reduced to two hours in keeping with international recommendations (footnote 2004)

APPOINTMENTS MADE

Regarding this assessment framework the following appointments are made:

- Institutions that are part of the financial core infrastructure[2] may use this framework by the implementation of their Business Continuity Management/Business Continuity Planning (BCM/BCP).

- DNB and the financial sector will jointly develop initiatives that on sector level will lead to an adequate attention of BCM/BCP.

Annex 1: Guidance regarding implementation continuity of the human factor for critical systems/business processes
Annex 2: An indicative list of relevant subjects that should be elaborated in a business continuity plan

[2] The financial core infrastructure consist of ABN AMRO Bank, Bank Nederlandse Gemeenten, Euroclear, Euronext, Fortisbank, Friesland Bank, F. Van Lanschot Bankiers, ING Bank, Equens, Kasbank, LCH.Clearnet SA, NIB Capital, Rabobank, SNS Bank and also De Nederlandsche Bank

ANNEX 1: GUIDANCE REGARDING IMPLEMENTATION CONTINUITY OF THE HUMAN FACTOR FOR CRITICAL SYSTEMS/ BUSINESS PROCESSES

The basic principle for this guidance is that the knowledge needed to ensure the operational continuity of systems/business processes guides the choice to make out of possible alternatives to ensure the continuity of the human factor (staff continuity). The matrix below shows this relation. In this matrix, the level of knowledge needed to keep systems/business processes, classified as critical, operational is set out on the left-hand scale, in decreasing order. The other scale presents the possible alternatives to ensure staff continuity.

Ways of ensuring staff continuity	*1. double staffing at another location*	*2. planned scheduling days off*	*3. shift work*	*4. use of staff from another location where a similar situation is operational*	*5. use of staff from another location where a similar situation is not operational*
Required level of knowledge of systems/business processes					
specific in the extreme (a)					*red*
highly specific (b)					
specific (c)					
not very specific (d)		*green*			
not specific (e)					

In the matrix, the green areas indicate minimally desirable options. If an option from a red area is chosen, a well-founded reason should be available.

The option chosen shows how the continuity of systems/business processes is ensured in the event of (temporary) unavailability of staff. It is essential that the measures aimed at ensuring staff continuity form part of the total package of measures intended to ensure the continuity of the most critical[3] systems/business processes.

In general, staff continuity in respect of such systems/business processes can be ensured by one of the following measures:

1. double staffing at another location;
2. by a planned scheduling of days off providing for the permanent external availability of sufficient and qualified staff (away from the location where the systems/business processes are operational);
3. shift work;
4. the use of staff at another location where similar systems/business processes are operational;
5. the use of staff from another location where similar systems/business processes are not operational.

As noted in the basic principle, the choice to be made with regard to the staff needed depends on the knowledge needed to keep the systems/business processes operational and/or on the position of the systems/business processes at the time of disruption. In this context, the various levels of knowledge needed are distinguished as follows:

[3] Critical are those systems/business processes which:

- are essential to the liquidity needs of the institution itself, its customers or financial institutions with which it maintains a (financial) relationship, and which, if disrupted, however minimally, could have serious negative consequences for the continuity of services provided by the institution, its customers or financial institutions with which it maintains a (financial) relationship:
- if disrupted as set out above, could have a considerable negative impact on the financial position of the institution itself, its customers or financial institutions with which it maintains a (financial) relationship.

a) specific in the extreme. Servicing by other staff at another location is no option;

b) highly specific. Similar systems/business processes are serviced by other staff at another location; they are well capable of taking over operations;

c) specific. Servicing by other staff at another location is an option, if they have been sufficiently trained in advance, and have gained sufficient relevant practical experience;

d) not very specific. Servicing by other staff at another location is an option if they have been sufficiently trained in advance;

e) not specific. Servicing by other staff, either own staff or externally recruited staff, at another location is an option. Prior training is not required.

With regard to **a)**, the following should be noted:

- where option 1 (double staffing) is concerned, it is recommended to operate the systems/business processes alternately from the primary and the alternative location. Where applicable, it is also advisable to exchange information about possible positions sufficiently frequently every day;
- where option 2 (planned scheduling days off) is concerned, it is recommended to make allowance for a prolonged breakdown. In this context, it is recommended to consider where it is possible:
    - to broaden knowledge of the systems/business processes via internal staff rotation. In the event of a prolonged breakdown, this staff could then function as back-ups;
    - to provide sufficiently knowledgeable extra staff via rapid recruitment and training for the longer-term. If this is possible, the plans and possible arrangements for the longer term should be laid down in writing.

- where option 3 (shift work) is concerned, the transfer time needed poses a risk. It is recommended to keep the transfer time between shifts as short as possible;
- a combination of option 2 (planned scheduling days off) and option 3 (shift work) may also be considered.

With regard to **b)**, the following should be noted:

- it is recommended to keep the critical systems/business processes operational alternately from the primary and the alternative location to ensure that the knowledge and experience of staff at both locations remain up to standard.

With regard to **c) and d)**, the following should be noted:

- it is recommended that the staff at the other location be properly trained and gain experience on a regular basis with keeping the systems/business processes operational. Active involvement of back-up staff in the execution of organisational disaster recovery tests allows them to gain experience and keep up knowledge.

With regard to **e)**, the following should be noted:

- here, the documentation needed for servicing is especially important. This aspect must be specifically addressed. Tests will need to show whether the available documentation is sufficient to help keep the systems/business processes operational without problems.

If, to ensure staff continuity, the option chosen is to let various staff gain knowledge and experience via job rotation and to mobilize them in the event of disasters to keep systems/business processes operational, it is recommended to adjust organisational measures such as access to systems and locations accordingly.

Where the qualification of systems/business processes is concerned, the critical nature of each system and/or process should be determined by a Business Impact Analysis (BIA). It is recommended that this analysis should indicate, among other things, the required servicing level, the components and resources needed for servicing (such as procedures, staff (number and knowledge level), office equipment, technical equipment, telecommunication arrangements, IT systems and applications, (system) software and supporting software tools). It is recommended to define, per critical system, an RTO (Recovery Time Objective), commensurate with the required servicing level. In view of the importance of critical systems/business processes, measures should be taken to ensure that these systems can be serviced at another location.

ANNEX 2: AN INDICATIVE LIST OF RELEVANT SUBJECTS THAT SHOULD BE ELABORATED IN A BUSINESS CONTINUITY PLAN

The following questions should be dealt with in a business continuity plan of an institution:

- What are the critical operating functions, processes and products?
- What is the business continuity strategy of the institution?
- What are the concrete business continuity objectives and measures and are they geared to the time that the systems/business is not expected to be able to function at the primary site (e.g. back-up centre operational within two hours)?
- Have the continuity plans been approved by senior management?
- What catastrophic event scenarios are described in them?
- Is there a back-up site (absolutely essential in the case of an LVPS, CCP or SSS)?
- What configuration requirements should the back-up site fulfil?
- What is the location of the back-up site?
- What measures exist to be able to staff the systems and business at a back-up site?
- What is the risk profile of the primary and secondary sites?
- How is the process of data replication arranged?
- To what extent is the company dependent on external providers?
- What procedures exist in order to be able to continue critical operating processes (e.g. settlement in the event of liquidity problems)?
- How is the outsourcing of activities arranged?
- What security and continuity requirements are made of the participants in the systems?
- What tests are made of the alternative sites?
- How is the crisis command and communication organised?
- Are the contact lists and procedures/checklists up to date?
- Are the continuity plans transparent and known in the market and to regulatory authorities/overseers and other authorities?
- Are the business continuity plans geared to international aspects (e.g. has account been taken of business activities in other countries)?