BACKGROUND OF THE DOMESTIC SURVEY

Unexpected incidents worldwide have focused the attention of the financial sector, including the participants of the domestic payment and settlement systems, **on the assurance of business continuity, and have raised this issue to a strategic level.**

External and internal threats can jeopardise the operation of financial institutions in the fulfilment of their role played in the economy and in meeting their obligations towards their clients by generating smaller or more significant service disruptions. Insufficient level of the activities that are critical for the economy may withhold the effectiveness of the financial sector and, in extreme case, may endanger the stability of the whole system due to the interconnectedness of the system participants. Hence, central banks around the world put an emphasis on the proper management of operational risks within the institutions that provide services of critical importance.

Central banks in the developed countries concern themselves with the business continuity practices of the financial sector since several years. Central banks and financial supervisions in these countries (UK, Italy, USA, Netherlands, Japan, Singapore, Switzerland, Australia, Hong Kong) continuously adjust and update their recommendations formulated based on regular survey and testing in the field of business continuity.

THE DOMESTIC SURVEY AND THE CONSEQUENT RECOMMENDATIONS

Article 4 (5) of the Act on the National Bank of Hungary sets out oversight as a fundamental role of the NBH, with the purpose of promoting the secure and effective functioning of the payment systems. The way this is put in practice is highly influenced by the individual practices of the system participants. This is the first time that a survey on business continuity took place in Hungary. Recent incidents worldwide and in Hungary, as well as an international tendency of oversight policies have justified scheduling the work now.

Paragraphs 13, 13/B- /C and /D of the Act CXII of 1996 on Credit Institutions and Financial Undertakings (hereinafter Banking Act) contain provisions on business continuity. These are audited by the State Supervision of Financial Institutions (hereinafter PSZÁF). PSZÁF has issued methodology guidance[1] on the protection of financial institutions' information systems. **PSZAF approaches business continuity from the perspective of the complete range of financial institutions' activity.** Hence, an extension of their approach is justified specifically for payment systems. On the other hand **PSZÁF's supervision does not fully cover the community of participants of the Hungarian payment systems,** not even the circle of critical participants.

[1] „Methodology guidance 1/2007. on the protection of financial institutions' information systems". Provisions on page 8. (risk analysis), pages 17-18. (ensuring continuity of services) and pages 20-21. (backups and archives) are essential for business continuity.

For the above reasons we have identified the critical participants of VIBER and BKR[2] according to their weight in the total payment turnover, and we stimulated common thinking in the topic of business continuity. As a first step we surveyed in the first half of 2010 the top 13 credit institutions and the State Treasury, weighing together 82,67% of the total domestic payment turnover. **Our goal was to overview the current business continuity preparedness of this narrower segment of the financial sector. The survey focused on the practices related to the provision of payment services and to the institutions' participation in the payment systems.**

Our survey covered the following topics:

- Business continuity strategy, management
- Business impact analysis (BIA), risk analysis
- Business continuity planning
- Fundamental resources for business continuity
    - Human resources
    - Primary and alternate sites
    - Infrastructure
    - Dependence on external service providers;
- Recovery and resumption objectives and plans
- Background solutions of critical operational processes and functions (alternate site)
- Testing of business continuity plans

The survey allowed us to draw a picture of the practice followed by the selected participants. A fundamental finding of the survey is that participants have without exception recognised the importance of business continuity and have developed fairly comparable measures to tackle the issue. Nevertheless, the preparedness of the domestic financial sector is lagging behind that of the institutions present in the world's leading financial centres. Besides, co-operation, common thinking, mutual preparation and joint testing are also not current practice.

We are fully aware that the development of a more uniform practice can be time- and resource consuming therefore we support a step-by-step approach on the participants' side. To help this process we publish **an oversight recommendation package for the payment system participants.** Our recommendations represent a uniform approach that can be used as guidance and along which the institutions can benchmark their strengths and weaknesses in the field of business continuity. When finalising the recommendations we have taken into consideration the remarks formulated by the banking community.

We trust that the work that was performed will result on the medium- and long run in further harmonisation and uniformisation of business continuity practices within the sector, hence reducing operational risks of the sector as a whole. Greater harmonisation will permit overall quicker and steadier reaction across the sector in case of eventual incidents or catastrophes.

The present oversight recommendations **aim at facilitating the transition of the business continuity concept in the area of payments into a sufficiently regulated, well documented, thorough but transparent in its context, practical activity, using optimal resources, that provides security to the financial sector.**

[2] VIBER: Hungarian RTGS, BKR: Hungarian retail payment system (sometimes also called „Giro")

OVERSIGHT RECOMMENDATIONS ON BUSINESS CONTINUITY

I. Business continuity strategy, management

I/1. recommendation: The firm should develop a business continuity strategy covering the business continuity and recovery activity of both the business areas and the information technology system. This should be approved at least by the executive senior management level.

I/2. recommendation: An organisational unit, preferably independent of the IT area, should be designated to be responsible for the comprehensive co-ordination of business continuity efforts.

Leading practice:

I/3. recommendation: It is useful, if business continuity efforts are co-ordinated under the direction of a business continuity committee comprising of the heads of the process owner business areas and senior managers of the firm.

II. Business impact analysis (BIA), risk analysis

II/1. recommendation: A business impact analysis (BIA) should be prepared, based on the business continuity strategy, and reviewed each year. The BIA identifies critical processes, assigns a process owner to each of these, specifies the critical resources, determines the vulnerability window of the processes, and expresses the value of the process or resource in money and in other terms from the firm's point of view.

II/2. recommendation: The BIA should be prepared according to uniform principles with the approval of the top management, at least in respect of the critical processes, the list of resources and the quantified business impact, . Application of the uniform principles should be supervised by the entity entrusted with the business continuity co-ordination.

II/3. recommendation: To complete the BIA, a risk analysis should be made, which explores the specific threats of the processes and the probability of their occurrence as well as the dependency of processes on resources. The risk analysis should also be updated annually.

II/4. recommendation: In case of new **critical** products or processes, the BIA and the risk analysis as well as the successful business continuity test of the product or process should constitute a precondition of the introduction (the same is valid if an existing product or process is changed).

Leading practice:

II/5. recommendation: The business impact of each individual threat is determined in precisely calculated money terms rather than according to limit amounts (bands). Accordingly, the weighting of individual processes becomes more precise.

II/6. recommendation: The BIA is prepared by dedicated software support used by each organisational unit.

III. Business continuity planning

III/1. recommendation: Firms should set up a business continuity plan and a disaster recovery plan for each critical process and resource identified in the BIA. Harmony between these plans must be ensured. Plans should be reviewed at least annually, and adjusted if necessary. In addition, review and adjustment is also required if the process or the resource changes significantly. Training and testing of the plans is performed in a documented manner once a year.

III/2. recommendation: Business continuity planning should address the backup procedures of the processes affected by the crisis and the recovery method of terminating the underlying reasons for the crisis.

III/3. recommendation: Lessons learned from incident management and the results of the business continuity tests should be incorporated in the business continuity plans without delay.

III/4. recommendation: The BCP documentation should be available in electronic and printed formats both at the primary and alternate sites.

III/5. recommendation: Internal audit should regularly cover the validity of the BCPs.

Leading practice:

III/6. recommendation: New **critical** products or processes or changes to existing **critical** products or processes should only be introduced once the backup solutions have been developed and successfully tested.

IV. Fundamental resources for business continuity

Human resources

IV/1. recommendation: Types of incidents and disaster situations that jeopardise the availability of staff (traffic, strike, epidemic etc.) should be listed out and business continuity procedures should be elaborated accordingly.

IV/2. recommendation: The minimum staff number and the key personnel should be determined for each organisational unit and critical process. Common knowledgebase and appropriate decision-making authority should be ensured to support their duties.

IV/3. recommendation: The long- and short-term solutions on staff substitution should be planned and assessed. It may be done by a central unit or at the level of each organisational unit, however in the latter case a central synthetic record should be available and access to the records by the appropriate stakeholders is required in any case.

IV/4. recommendation: Key individuals should be identified and a plan should exist for their replacement or substitution., The plan should include the designation of alternates (background personnel), the methodology of their cross-training, the creation of a knowledge base supporting the substitution and the rules of participation in the tests.

IV/5. recommendation: The issues of minimum staff necessary for ensuring the critical processes, key personnel and substitutes (order of substitution) must continuously be monitored and updated at the firm's every organisational change and in case of changes in critical processes. An adjustment is also required upon each lesson learned from incident management, as a result of business continuity tests and whenever business continuity processes are revised.

IV/6. recommendation: There should be assurance that the background personnel and alternates have access to the relevant systems and databases.

IV/7. recommendation: A senior manager or a manager with appropriate decision-making authority, able to exercise control in an emergency, has always to be available.

IV/8. recommendation: Signatories should be redundant to ensure that the firm is adequately represented in an emergency.

IV/9. recommendation: It is useful to assess to what extent of the planned business continuity processes are able to tolerate the shortage of staff. Similarly, an assessment of how long the backup solutions can be maintained for in the daily course of business can be of use.

Primary and alternate sites

IV/10. recommendation: To ensure business continuity in respect of their critical processes and functions, firms should have alternate sites (IT and workplace).When setting up an alternate site care must be taken to locate the two sites geographically at a distance that ensures a fundamental difference between their risk profiles.

IV/11. recommendation: The following backup resources and devices should be available at the alternate site:

- generator/uninterruptible power supply necessary for the operation of the systems;
- air-conditioning equipment necessary for cooling the equipment, demister;
- computers of adequate capacity necessary for performing the critical processes;
- business computer programmes necessary for pursuing the critical business activity;
- secure remote data communication devices (which allow confidentiality, integrity and credibility of the data transmission);
- up-to-date documentation of work procedures and IT operations.

IV/12 recommendation: In case the sites (either the primary or the alternate or both) are located abroad, the domestic firm has to design the connectivity to the remote sites in a way to ensure access even in an emergency.

Leading practice:

IV/13. recommendation: Practice is considered leading if there is enough room at the alternate site to accommodate the personnel. Besides, there is appropriate equipment (e.g. desk, telephone, fax other office equipment) as well as water available for the critical staff to resume the critical business processes.

IV/14. recommendation: Practice is considered leading if the domestic firm is given the contractual right of on-site audit with regard to the provision of the service at the foreign entity providing the site abroad.

Infrastructure

IV/15. recommendation: The dependency of the alternate site on the primary site's critical infrastructure components should to be reduced to a minimum in order to ensure that the recovery time objectives set forth in the scenarios are achievable.

IV/16. recommendation: Ensuring redundancy, alternative supply chains and alternative service providers.

Dependence on external service providers

IV/17. recommendation: For all critical processes the dependences on external service providers/partners should be assessed.

IV/18. recommendation: In the case of critical processes, contracts, outlining the required service level, should be put in place with the external service providers. The agreements should be adjusted in case the business continuity strategy, the business processes and the relevant business continuity plans change.

IV/19. recommendation: The SLA should derive from the BIA in a way that the recovery and resumption objectives identified in the business continuity and disaster recovery plans are not jeopardized. The resultant of the SLAs of the services supporting the critical processes should be in accordance with – and should support – the expected availability determined in the vulnerability window of the critical process.

Leading practice:

IV/20. recommendation: The firm should have a copy of the external service providers' current, latest business continuity plans for the identified dependency relations.

IV/21. recommendation: Consistency of the external services providers' business continuity plans and the firm's own business continuity plans should be checked and ensured.

V. Recovery and resumption objectives and plans

V/1. recommendation: Recovery and resumption objectives should be identified for the critical operational processes and activities, and essentially for IT technology supporting them.. Documented testing should be performed to prove that recovery and resumption is achievable within the targeted period of time. Based on test results the business continuity and disaster plans should be adjusted.

V/2. recommendation: The defined recovery and resumption times should take into account the time need of the redirection /changeover/relocation to the alternate site . Consistency of these factors should continuously be ensured.

V/3. recommendation: There should also exist a planned process for switching /changing back/relocation from the alternate site to the primary site . The time requirement of the process should be assessed.

V/4. recommendation: Efforts should be made to recover the critical functions within the same settlement day.

V/5. recommendation: Recovery and resumption procedures should ensure that no loss of data and duplication occurs. Procedures should be tested (e.g. interruption test – redirection to the alternate site during the day in a way to create data gaps,[3] the processing of which should result in no loss or duplication of data).

VI. Background solutions of critical operational processes and functions (alternate site)

VI/1. recommendation: The alternate site should be designed in a way to allow the conducting of critical activities and processes.

VI/2. recommendation: The capacity of the alternate site may be lower than that of the primary site, but the minimum requirement is that in the case of a changeover the alternate site should be able to process the data mass of an average day. The capacity of the alternate site should be tested and the test documented.

VI/3. recommendation: After redirection of critical processes to the alternate site the firm should be able to close a business day at the alternate site and open the next business day at the alternate site.

[3] Incomplete series of operations

VI/4. recommendation: A technical description of the alternate site, continuously kept up to date, covering all devices and resources (network, set of appliances, configurations etc.) should exist and be available both at the primary and alternate sites in electronic format as well as in hard copy. Adjustment of and staff training on this documentation and should be part of business continuity efforts.

VI/5. recommendation: For cost-efficiency reasons, a bilateral business continuity agreement about using one another's primary sites as alternate site may be concluded with another firm. Shared alternate sites used by several participants may also be applied. In such cases, appropriate contractual conditions should guarantee that the operator of the shared site can in fact make the site available at the time of a business continuity event (incident), even if an incident affects several participants at a time.

Leading practice:

VI/6. recommendation: Leading practice is if the alternate site is able to process even the turnover of peak days or if the processing capacities of the two sites are identical.

VII. Testing of business continuity plans

VII/1. recommendation: A complete testing of the business continuity plans should be conducted at least once a year with regard to the critical processes and critical resources. Testing of business and IT aspects should be conducted concurrently, if possible. Critical processes that are interrelated or based on one another should preferably be tested jointly.

VII/2. recommendation: Each test result should be forwarded to the heads of the areas concerned as well as to the organisation or committee responsible for the co-ordination of business continuity and, at least in the form of a summary, to the senior management of the firm.

VII/3. recommendation: In case a firm outsources any part of its critical processes, it should become familiar with the business continuity procedures of the service provider and their test results, at least where the outsourcing is done within the firm's own company group . The firm should have adequate contractual assurance defined in a service level agreement for the enforcement of its interests.

VII/4. recommendation: Actual incidents and crises should be considered as spontaneous tests of the business continuity plans and should be treated accordingly in the business continuity procedures.

VII/5. recommendation: The inherent risks of the primary and alternate sites' differences in architecture, capacity and other aspects should be made transparent to the executive senior management, which has to approve them officially.

Budapest, 15 December 2010.

MAGYAR NEMZETI BANK