



**Business Continuity System
for the National Depository for Securities**

**Master Document
(abstract)**

Warsaw, 10 April 2006

CONTENTS

| | | |
|-----------|---------------------------------------------------------------------------------------------|----------|
| 1. | INTRODUCTION..... | 3 |
| 2. | BCS DOCUMENTATION..... | 3 |
| 3. | BCS GENERAL PRINCIPLES..... | 4 |
| 3.1. | APPLICABILITY | 4 |
| 3.2. | PROCESSES | 4 |
| 3.3. | RECOVERY TIME, REINSTATEMENT OF OPERATIONS AT THE PREMISES OF THE NATIONAL DEPOSITORY | 5 |
| 4. | BCS COMPONENTS | 5 |
| 4.1. | BACK-UP LOCATION | 6 |
| 4.2. | EMERGENCY CENTRE | 6 |
| 4.3. | RECOVERY TEAM..... | 7 |
| 4.4. | OPERATIONAL TASKFORCE..... | 7 |
| 4.5. | OPERATIONAL PROCEDURES..... | 7 |
| 4.6. | PROCEDURES FOR THE RECOVERY OF ORGANISATIONAL UNITS..... | 7 |
| 4.7. | EMERGENCY TESTING..... | 8 |
| 5. | GENERAL PRINCIPLES GOVERNING THE CONDUCT IN EMERGENCY..... | 8 |

1. Introduction

Deterioration in the standard and reliability of services caused by *force majeure* events (accidents or intentional conduct, natural disasters, etc.) may result in disruptions in the operation of the market and discontinuity in the provision of certain services to market participants, which may lead to loss of both domestic and foreign investor confidence.

With a view to minimising the operational risk to which the National Depository is exposed, a Business Continuity System (BCS)¹ has been developed, which consists of technical and organisational measures enabling the maintenance of the continuity of, or promptly restore, critical business processes following a serious breakdown or disaster, and to minimise the impact of the failure on the operations of the National Depository and other capital market institutions.

2. BCS Documentation

The BCS Documentation includes the following components:

- Master Document;
- Recovery Plan;
- procedures for the restoration of organisational units.

The Master Document includes general information concerning the BCS, its rules and components.

The Recovery Plan comprises a descriptive section which includes general information, a description of critical points and an algorithm according to which the operations of the National Depository are restored in emergencies, as well as procedures governing how the National Depository should be prepared to act in emergencies. Procedures for the restoration of organisational units outlines in detail how to prepare for the recovery of certain business processes.

The Master Document and the descriptive section of the Recovery Plan, as well as any modifications, are subject to approval by the National Depository Management Board.

An electronic version of the Master Document and the descriptive section of the Recovery Plan should be made available for Depository employees via the intranet.

Electronic versions of all procedures of the Recovery Plan and the procedures for the restoration of organisational units should be made available via the intranet for all Depository employees - members of the Recovery Team and the Operational Taskforce.

An abstract of the Master Document should be made available via the Internet.

¹ System Zachowania Ciągłości Funkcjonowania (SZCF)

The entire BCS documentation should be reviewed at least once a year. The review is conducted by the Department for Corporate Security, following which conclusions must be submitted to the Emergency Centre.

3. BCS general principles

3.1. Applicability

The BCS has been developed to address two types of short- or long-term emergencies, generally defined as:

- a failure of IT processing systems located in the premises of the National Depository as a result of which back-up systems must be used;
- prevention of use of the premises of the National Depository.

The first type involves a situation in which, generally speaking, at least one of the following is unavailable:

- the central processing system defined as all central units necessary for the execution of business processes;
- communication systems used in the premises of the National Depository;
- external facilities (e.g. data transfer, telephone lines);
- supply of public services which are indispensable to the operation of the systems (such as power and water supply).

The second type involves a situation in which the primary location is unavailable or cannot be used, which may be caused for instance by a terrorist attack, fire, public services outages, etc.

Detailed procedures are included in the Recovery Plan.

The BCS does not address global emergencies such as natural disasters and external services outages affecting the entire system (e.g. failures of domestic or inter-bank data transfer telecommunications systems or telephone lines) which are beyond the control of the National Depository, in which case the provisions of law or procedures agreed with external partners on a separate basis should apply.

Moreover, the BCS does not address situations involving problems with the execution of certain business processes or minor technical defects, to which operational procedures of individual organisational units of the Depository should apply.

3.2. Processes

For the purposes of the BCS, the processes executed at the National Depository have been categorised into:

- critical processes;
- secondary processes.

Critical processes are those whose performance by a specific date and in a specified manner has a significant impact on the functioning of the National Depository (execution of statutory duties, legal obligations, financial covenants) and capital market institutions subordinated to the Depository, and which, if unexpectedly discontinued, result in material consequences in the form of financial costs or loss of credibility. Those processes are covered by the National Depository Operational Risk Management Model.

All other processes executed at the National Depository, whose performance may be delayed without adversely affecting the National Depository's business functions and without the Depository being legally or financially liable, are defined as **secondary** processes.

3.3. Recovery time, reinstatement of operations at the premises of the National Depository

According to the BCS, a non-extendible recovery time of critical processes is 4 hours, whether in the primary premises or in the back-up location of the National Depository.

The BCS does not impose an obligation to restore secondary processes during the same Depository business day in which the emergency has occurred. In the case of a long-term non-availability of the premises of the Depository, secondary processes should be reinstated, as required, within 1-5 business days, in the back-up location or other premises outside the National Depository.

Detailed procedures are included in the Recovery Plan.

After the emergency has ended, the operations of the National Depository should be fully reinstated in its premises. In general terms, the following mode of reinstating the premises of the National Depository has been established:

- in the case of a prior inability of using the premises resulting in the transfer of employees to the back-up location, employees should return on the first Depository business day after the reasons for the transfer of employees have been removed;
- in the case of a prior failure of IT processing systems or after a scheduled use of back-up systems, the return to production systems should be carried out during the first weekend after the failure has been removed or the relevant decision has been taken.

4. BCS components

In the course of its development, the following components of the BCS have been established:

- Back-Up Location;
- Emergency Centre;
- Recovery Team;
- Operational Taskforce;
- operational procedures;
- procedures for the restoration of organisational units;
- emergency testing.

4.1. Back-Up Location

For the purposes of assuring business continuity in emergencies, the National Depository has its own back-up location. In order to avoid a situation in which both the primary premises and the back-up location are unavailable at the same time, the latter is located outside the capital city of Warsaw.

In order to ensure the continuity of business processes, the back-up location has been equipped with:

- replicas of all production IT systems;
- the necessary number of workstations, as required by the definitions of the executed processes;
- the necessary technical and office equipment;
- an exclusively owned permanent data link with the primary premises, with a capacity enabling a real-time transfer of all production data;
- an exclusively owned permanent telecommunications connectivity with market participants and the Internet;
- an exclusively owned telephone exchange;
- an exclusively owned backup power supply system;
- the necessary facilities for employees.

4.2. Emergency Centre

As part of the Business Continuity System, an Emergency Centre has been formed by the National Depository Management Board, the responsibilities of which include:

- coordinating all activities of the National Depository if an emergency occurs and the Recovery Plan is launched;
- analysing changes taking place in the National Depository and its business environment and modifying the BCS documentation accordingly;
- coordinating the updating of the procedures for the restoration of organisational units of the National Depository;

- analysing the operational security of the National Depository and submitting recommendations to the National Depository Management Board;
- BCS testing (planning and execution);
- coordinating all the activities necessary to assure that the Back-Up Location is put on standby to take over the functions of the primary premises of the National Depository;
- BCS training (planning and execution).

In order to accelerate the recovery of the National Depository operations in emergencies, the Emergency Centre acts as a decision-maker in the process of restoring the business operations of the National Depository and launching the execution of Recovery Plan procedures.

The responsibilities of the members of the Emergency Centre in the event of an emergency are detailed in the Recovery Plan.

4.3. Recovery Team

As part of the BCS, a Recovery Team has been established which is responsible for a prompt set-up of the critical back-up IT systems immediately in the event of an emergency and, if necessary, for preparing the back-up location for the recovery of National Depository business operations.

4.4. Operational Taskforce

The Operational Taskforce is composed of the employees of the organisational units covered by the BCS. The Taskforce is responsible for restarting individual workstations in the back-up location, controlling the degree to which business processes are performed and the status of applications and informing the National Depository's partners and employees of the emergency.

Once the stage of analysing the process and system status has been completed, the members of the Operational Taskforce restore business processes covered by the BCS.

4.5. Operational procedures

All processes executed at the National Depository should be described in the relevant operational procedures. Electronic versions of the operational procedures are stored in the National Depository network system and should be made available to those employees of the Depository who are involved in their execution. The Recovery Plan includes a list of operational procedures and information as to the location of those procedures.

4.6. Procedures for the restoration of organisational units

In addition to operational procedures governing all processes executed by organisational units of the National Depository, a recovery procedure should be in place to regulate the detailed manner in which the recovery of the business process concerned should be prepared.

Electronic versions of the procedures are stored in the National Depository network system and should be made available to those employees of the Depository who are involved in the recovery of the processes. The Recovery Plan includes a list of recovery procedures and information as to the location of those procedures.

4.7. Emergency testing

All BCS components should be regularly tested. The BCS testing should be conducted at least twice a year, including once a year in cooperation with the institutions operating in the capital market. In addition, any changes to the BCS rules as well as the most far-reaching modifications to the IT technology must be tested in-house.

5. General principles governing conduct in emergencies

The Master Document includes information as to the mode of conduct in emergencies, which is generally defined as:

- a failure of IT processing systems located in the premises of the National Depository, as defined under section 3.1 above, as a result of which any of the back-up systems located in the back-up location must be used;
- non-availability of the premises of the National Depository, including in particular if these must be evacuated or if operations may not be continued in the premises.

Detailed emergency procedures are included in the Recovery Plan.