



The National Depository for Securities

Business Continuity System for the KDPW Group

Master Document – BCS Policy

(abstract)

Warsaw, 18 January 2012

Contents

1. Introduction.....	3
2. BCS general principles	3
2.1. Applicability.....	3
2.2. Processes.....	4
2.3. Recovery time, reinstatement of operations at the premises of the KDPW Group.....	4
3. BCS Documentation	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. General recovery procedures.....	7
4.6. Recovery procedures of the organizational units.....	7
4.7. Operational procedures of the organizational units	7
5. General principles governing conduct in emergencies.....	8
6. BCS testing.....	8
7. Maintenance and development of BCS	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 disruption 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 minimizing the operational risk to which the KDPW Group is exposed, a Business Continuity System (BCS) has been developed, which consists of technical and organizational measures enabling the maintenance of the continuity of, or promptly restore, critical business processes following a serious breakdown or disaster, and to minimize the impact of the failure on the operations of the KDPW Group and other market institutions.

2. BCS general principles

2.1. Applicability

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

- a failure of IT processing system located in the premises of the KDPW Group as a result of which back-up system must be used;
- prevention of use of the premises of the KDPW Group.

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 system used in the premises of the KDPW Group;
- external facilities (e.g. data transfer, telephone lines);
- supply of public services which are indispensable to the operation of the system (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 disaster and external services outages affecting the entire system (e.g. failure of domestic or inter-bank data transfer, telecommunications systems or telephone lines) which are beyond the control of the KDPW Group in which case the provision of law or procedures agreed with external partners on a separate basis should apply.

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

2.2. Processes

For the purposes of the BCS, the processes executed in the KDPW Group have been categorized into:

- critical processes;
- supporting processes;
- secondary processes.

Critical processes are those whose performance by a specific date and in a specific manner has a significant impact on the functioning of the KDPW Group (execution of statutory duties legal obligation, financial covenants) and capital market institution subordinated to the KDPW Group, and which, if unexpectedly discontinued, result in material consequences in the form of financial costs or loss of credibility.

Supporting processes are those whose performance is necessary for the full execution of critical processes.

All other processes executed in the KDPW Group, whose performance may be delayed without adversely affecting the business functions and without the KDPW Group being legally or financially liable are defined as secondary processes.

2.3. Recovery time, reinstatement of operations at the premises of the KDPW Group

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 KDPW Group.

The execution of supporting processes should be restored on the same business day.

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

Detailed procedures are included in the Recovery Plan.

After the emergency has ended the operations of the KDPW Group should be fully reinstated in its premises. In general terms, the following mode of reinstating the premises of KDPW Group 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 KDPW Group 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 system should be carried out during the first weekend after the failure has been removed or the relevant decision has been taken.

3. BCS Documentation

The BCS Documentation includes the following components:

- Master Document – BCS Policy;
- Recovery Plan;
- recovery procedures of the organizational units;
- operational procedures of the organizational 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 KDPW Group are restored in emergencies, as well as procedures governing how the KDPW Group should be prepared to act in emergencies. Procedures for the restoration of organizational 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 for Securities (KDPW) Management Board.

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

Electronic version of all procedures of the Recovery Plan and the procedures for the restoration of organizational units should be made available via the Intranet for all KDPW Group employees - members of the Recovery Team and the Operational Taskforce.

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

The entire BCS documentation should be reviewed at least once a year, or whenever any major changes appear in KDPW Group or its business environment. The review is conducted by the Corporate Security Department of the National Depository for Securities (KDPW).

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;
- general recovery procedures;
- recovery procedures of the organizational units;
- operational procedures of the organizational units.

4.1. Back-up Location

For the purposes of assuring business continuity in emergencies, KDPW Group 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 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 system;
- the necessary number of workstations, as required by the definitions of the executed processes;
- the necessary technical and office equipment;
- 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 for Securities (KDPW) Management Board, the responsibilities of which include:

- coordinating all activities of the KDPW Group if an emergency occurs and the Recovery Plan is launched;
- analyzing changes taking place in the KDPW Group and its business environment and modifying the BCS documentation accordingly;
- coordinating the updating procedures of the restoration of organizational units of the KDPW Group;
- analyzing the operational security of KDPW Group and submitting recommendations to the National Depository for Securities (KDPW) Management Board;
- 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 KDPW Group;
- BCS training (planning and execution).

In order to accelerate the recovery of the KDPW Group operations in emergencies, the Emergency Centre acts as a decision-maker in the process of restoring the business operations of the KDPW Group 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 KDPW Group business operations.

4.4. Operational Taskforce

The Operational Taskforce is composed of the employees of the organizational units covered by 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 KDPW Group partners and employees about the emergency.

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

4.5. General recovery procedures

The general recovery procedures describe the mode of conduct in emergencies. The Recovery Plan includes a list of general recovery procedures and information as to the location of those procedures.

4.6. Recovery procedures of the organizational units

The recovery procedures 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 KDPW Group network system and should be made available to those employees of the KDPW Group 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. Operational procedures of the organizational units

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

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 KDPW Group, 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 KDPW Group, 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.

6. BCS 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 financial 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.

7. Maintenance and development of BCS

The results of operational tests, reviews of BCS documentation and published standards, and analysis of the impact of operational changes in the KDPW Group and in its business environment on the risk profile are the basis for optimizing and developing actions ensuring the desired effectiveness of BCS.

In case of an incident causing the necessity of launching the Recovery Plan it is required to perform “after the incident” review in order to assess:

- the correctness of identification and classification of event and its impact on operational activity of KDPW Group;
- the adequacy of actions performed by the Emergency Center;
- the effectiveness in achieving the objectives of BCS, including the recovery time;
- the competence of staff performing tasks within BCS.

The review report can be the basis for recommended corrective actions and possible changes in BCS guidelines.