25 October 2017

KDPW
KDPW | CCP

Business Continuity Planning System for the KDPW Group - BCP System Policy (excerpt)

Contents:

I. Introduction 2

II. BCP System general principles 2

III. BCP System Documentation 4

IV. BCP System operational resources 4

V. General procedures in the event of emergencies 6

VI. BCP System testing 6

VII. BCP System review 7

VIII. Maintenance and development of BCP System 7

I. Introduction

The loss of the high standard and of the timeliness of services provided by the KDPW Group as a result of adverse operational conditions, may lead to disruptions in the financial market, which may in turn lead to loss of revenues and affect the corporate reputation of the companies belonging to the KDPW Group and its stakeholders.

In order to minimise the impact of incidents and disruptions on the business operations of KDPW and KDPW_CCP and its business partners, a Business Continuity Planning (BCP) System has been introduced within the Group, as a range of technical and organisational processes established to enable the maintenance – in the event of a serious emergency or disaster – of business continuity or to ensure the fastest possible recovery time for core business processes while lessening the impact of the incident on operations of the KDPW Group and of other financial market institutions.

II. BCP System general principles

The purpose and scope of the BCP System derive from the analysis of the impact of potential disruptions on the operations of the companies belonging to the KDPW Group, based on the assessment of operational risk within the Group.

II.1. Application

The BCP System has been prepared in the event of short-term or long-term emergencies of two types, which may be broadly described as follows:

1) An IT systems failure in the primary Group business site, which may result in the need to deploy back-up systems;
2) The Group's primary business site is incapacitated.

The first variant relates to a situation where at least one of the following elements is unavailable:

1) The central processing system within the meaning of IT solutions necessary to execute business processes;
2) Communication systems processing the Group's primary business site;
3) External services provided locally (e.g. data transfer, telephone communication);
4) Provision of essential utilities for systems to operate locally (e.g. electricity, water).

The second variant involves circumstances where the primary business site is inaccessible or cannot be used as the result of a threat of terrorist attack, fire or pollution.

Detailed procedures executed in the abovementioned situations are contained in the Business Recovery Plan.

The BCP System excludes provision for global emergencies, such as natural disasters and disruptions in external services broadly affecting the whole system (e.g. national or global disruption in telecommunication), over which the KDPW Group has no control. In such circumstances, provisions of law, or procedures agreed with external service providers on the basis of separate measures should apply.

Moreover the BCP System does not cover situations involving disruptions in the execution of separate business processes, or minor technical problems, where the operational procedures of specific KDPW Group organisational units should apply instead.

II.2. Processes

For the purposes of the BCP System, the business processes performed in the companies belonging to the KDPW Group have been divided into three categories:

1) Critical processes;
2) Support processes;
3) Ancillary processes.

Critical processes are processes whose performance within a set time and in a pre-determined manner have a significant impact on the business operations of the companies belonging to the KDPW Group (achieving corporate goals set out in the company statute, obligations deriving from provisions of law and contractual agreements, financial obligations) as well as on other financial market entities, whose business activities are dependent on the operations of the KDPW Group and whose unintended disruption may result in severe adverse consequences, in particular including financial costs, breach of laws or loss of professional standing.

Support processes are processes, whose performance is necessary for critical processes to be fully realised, but they are not the main actions result in realisation of critical processes.

All remaining processes performed within the companies belonging to the KDPW Group, whose realisation may be delayed without causing any significant impact on the business functions carried out by the KDPW Group, or without leading to legal or financial consequences for the KDPW Group, shall be assigned the status of **ancillary** services.

II.3. Recovery parameters

The BCP System sets a Recovery Time Objective (RTO) for **critical processes** at **2 hours**, which is the maximum time from the occurrence of a contingency until the process is re-sumed, irrespective of the recovery location (KDPW Group head office, KDPW Group Business Recovery Site or other location outside Group head office).

The recovery of **support processes** should take place before the end of the relevant business day.

The BCP System does not envisage recovery of **ancillary processes** on the same business day that the emergency took place. In instances where it is expected that long-term access to the KDPW Group head office will not be possible, recovery of ancillary processes shall be determined on the basis of need within 1-5 business days in the business recovery site, or another site outside KDPW business head office, while at the same time taking account of the possibility of employees “working remotely”.

The Business Recovery Plan contains detailed rules for the recovery of critical and support processes.

Following the end of the emergency, full recovery of business activities by the companies belonging to the KDPW Group should take place in the KDPW Group head office. In general, the return to the head office shall take place according to the following principles:

1) In circumstances where the corporate head office has become inaccessible, resulting in the transfer of employees to the business recovery site, their return to the head office shall take place on the first KDPW Group business day following the elimination of the cause of the transfer of employees;

2) In the event of a prior IT systems failure, or following a planned launch of back-up systems, the transfer back to processing using main production systems shall take place on the first weekend following the elimination of the cause of the disruption.

III. BCP System Documentation

BCP System Documentation includes the following elements:

1) BCP System Policy;
2) The Business Recovery Plan and the general recovery procedures;
3) Recovery rules for organisational units;
4) Operational procedures for organisational units .

BCP System Policy includes general information concerning the BCP System, its rules and components.

The Business Recovery Plan consists of a description, containing general information, an overview of essential elements and an algorithm for the business recovery of companies belonging to the KDPW Group in the event of an emergency, appendices and general recovery procedures relating to instructions on preparing the KDPW Group for maintaining operations in an emergency.

The recovery rules for organisational units relate to detailed rules of procedure whose purpose is preparing for the recovery of specific business processes in each organisational unit of companies belonging to the KDPW Group.

Operational procedures for organisational units relate to standard rules of procedure in specific business processes of organisational units of companies belonging to the KDPW Group taking part in the realisation of these processes.

Changes of the BCP System Policy and the descriptive section of the Recovery Plan agreed between KDPW S.A. and KDPW_CCP S.A. should be approved by the KDPW S.A. Management Board and the KDPW_CCP S.A. Management Board, respectively. The Directors of the organisational units shall be responsible for ensuring that the rest BCP System Documentation are up to date.

IV. BCP System operational resources

The BCP System consists of the following separate components:

1. The Business Recovery Site;
2. The Crisis Response Group;
3. The Recovery Unit;
4. The Operational Group;
5. General recovery procedures;
6. Recovery procedures for organisational units;
7. Operational procedures for organisational units;

IV.1. The Business Recovery Site

In order to ensure business continuity in the event of emergencies, KDPW Group retains its own business recovery site, which is located outside the Warsaw city limits, in order to prevent situations where the primary business site and the business recovery site should both become inaccessible. The companies belonging to the KDPW Group use this site.

In order to ensure the continuity of business processes of the companies belonging to the KDPW Group, the business recovery site has been equipped in particular with the following:

1) back-ups of all IT production systems;
2) essential number of staff posts corresponding to the designation of company business processes being realised;
3) essential technical and office equipment;
4) a fixed telecommunication link, owned by KDPW, connected with the KDPW Group primary business site and holding sufficient capacity to transfer all production data online;
5) fixed links access to telecom operator services;
6) its own telephone exchange;
7) its own emergency power supply;
8) essential social facilities.

IV.2. The Crisis Response Group

As part of the Business Continuity Planning System, the Crisis Response Group is established whose duties include in particular:

1) Analysis of the impact of an existing event on KDPW Group business operations;
2) Initiation of the Business Recovery Plan and coordination of all activities of the companies belonging to the KDPW Group in relation to business continuity management in the event of an emergency;
3) Analysis of the security level of KDPW Group operations and submitting relevant observations to the Management Boards of the KDPW Group.

In order to accelerate the recovery of the KDPW Group operations in emergencies, the Crisis Response Group acts as a decision-maker in the process of restoring the business operations of the KDPW Group and launching the execution of Business Recovery Plan procedures.

The responsibilities of the members of the Crisis Response Group in the event of an emergency are detailed in the Business Recovery Plan.

IV.3. The Business Recovery Unit

The Business Recovery Unit is comprised of designated employees from the KDPW IT Systems Department. The role of the Business Recovery Unit is to make immediate preparations – as soon as possible following the start of an emergency – for the deployment of essential back-up IT systems, and if necessary, to prepare the business recovery site for the recovery of KDPW Group business processes, depending on the crisis management strategy approved by the Crisis Response Group.

IV.4. The Operational Group

The Operational Group consists of designated employees from each organisation unit of companies belonging to the KDPW Group, whose business processes are covered by the BCP System.

The role of the Operational Group is to initiate the creation of specific staff posts in the business recovery site, to monitor the level of completion of business processes and the state of applications, as well as to inform outside parties and employees of companies be-longing to the KDPW Group of the emergency situation, which has arisen.

Following the completion of the status analysis of processes and systems, members of the Operational Group commence the recovery of each business process covered by the BCP System.

IV.5. General recovery procedures

The general recovery procedures describe the measures to be undertaken as part of crisis management and they form an appendix to the Business Recovery Plan which contains a list of archived general recovery procedures and their location in the KDPW Group IT network.

IV.6. Recovery procedures for organisational units

Each business process performed by the KDPW Group and included in the BCP System will require a corresponding recovery procedure relating to detailed rules of measures to be undertaken in order to plan for the recovery of a given business process and its continuation in accordance with operational procedures.

The operational procedures should be submitted in electronic form in the KDPW Group IT system and be made available to employees of the companies belonging to the Group involved in the recovery of processes. The KDPW Group Business Recovery Plan contains a list of archived recovery procedures and their location in IT network.

IV.7. Operational procedures of the organisational units

The rules for the performance of all business processes carried out within the KDPW Group, which are covered by the BCP System, should be described in the relevant operational procedures.

Operational procedures should be archived in electronic form in the KDPW Group IT system and be made available to employees of the Group involved in their performance. The KDPW Group Business Recovery Plan contains a list of archived operational procedures and their location in IT network.

V. General procedures in the event of emergencies

The model of conduct of the companies belonging to the KDPW Group in emergencies is created on two basic types of events generally defined as:

1) a failure of IT processing systems in the KDPW Group primary business site, resulting in the need to utilise one of the back-up systems located in the business recovery site;
2) inaccessibility of the KDPW Group head office, including in particular if these must be evacuated or if operations may not be continued in the primary business site.

Detailed algorithms to be undertaken in order to the above mentioned situations are included in the Business Recovery Plan.

VI. BCP System testing

Comprehensive BCP System tests which check the readiness of the KDPW Group for operation in a crisis should be performed at least twice per year, including tests in co-operation with other financial market institutions performed at least once per year. Moreover, every significant change in the area of business activities of the companies belonging to the KDPW Group, or of the business environment, and all major changes relating to technology within the IT environment will require testing of the relevant BCP System to be performed.

VII. BCP System review

The BCP System documentation should be reviewed and verified. The review is conducted at least once a year, or whenever any major changes appear in KDPW Group.

The review of the BCP System generally incorporates other elements related to the operational risk management system of the KDPW Group.

VIII. Maintenance and development of BCP System

The results of tests and review of BCP System documentation, the publication of standards as well as implemented legislation, performed operational risk analyses, and analyses of the impact that operational changes taking place in the KDPW Group and its business environment may have on the level of the Group's operational security, all form the basis for measures to improve and develop the BCP System, ensuring that it meets the required standard of efficiency.
In the event of an emergency requiring the Business Recovery Plan to be put into effect an additional review is required in order to evaluate:

1) the correct identification and classification of the event and its effect on the business operations of the KDPW Group;
2) whether the Crisis Response Group is performing its duties in the correct manner and all other processes are executed in a crisis;
3) whether the goals of the BCP System have been effectively met, including recovery time;
4) the skills of the employees carrying out their responsibilities as part of the BCP System.

A report from a review of the evaluation procedure forms the basis for potential amendments to the general principles of the BCP System or for taking the necessary remedial action.