Foundations of Management, Vol. 2, No. 2 (2010), ISSN 2080-7279
DOI: 10.2478/v10238-012-0031-x

BUSINESS CONTINUITY

Janusz ZAWIŁA-NIEDŹWIECKI

Faculty of Management
Warsaw University of Technology, 02-524 Warszawa, Poland
email: jzawila@poczta.onet.pl

Abstract: Improving organization means on the one hand searching for adequate product (service) matched to the market, on the other hand shaping the ability to react on risks caused by that activity. The second should consist of identifying and estimating types of risk, and consequently creating solutions securing from possible forms of it's realization (disturbances), following rules of rational choice of security measures as seen in their relation to costs and effectiveness. As to types of risks from which the organization is not secure, the procedure left is to create plans for securing continuity of operations which ensure return to previous state in due course and ensuring replacement operations for the transitory period. Activities of creating the security measures and continuity solutions should be organized as constantly developing and perfecting and as such they need formal place in organizational structure and rules of management.

Key words: operational risk management, business continuity management.

1 Introduction

Ensuring business continuity encompasses:

- mechanism of reaction for disruptions of an organization (partly based on homeostasis, that is, spontaneous reaction of organization elements, and on systematically developed and studied ability to react), which consists in formation of the organizational skill of reacting to disruptions,
- process of development of the above mentioned ability to react to disruptions (as a supporting process for core organization activity, from the point of view of process analysis),
- process of managing the current ability of ensuring business continuity and its constant development.

Disruption reaction mechanism consists of:

- organizational structure dedicated to ensuring business continuity being an integral part of the general organizational structure,
- formal organizational regulation determining relations in the organizational structure connected to the task of ensuring business continuity,
- established practice (possibly written) of actions in situations when reaction to disruption, which has appeared, is required.

It is particularly important to underline, that reaction to disruption viewed as ensuring business continuity should be understood not only as direct action in the face of disruption, but also as preventive activity connected with analysis of threats and weaknesses and search for solutions and methods of averting the occurrence of threats. In this sense, the efforts towards business continuity and safety interlace with one another. From the point of view of business continuity, the safety solutions ensure prevention against threats, while from the point of view of safety, the business continuity solutions constitute a good insurance, in case other safety means fail to work properly (see Figure 1). This supports the concept of managing both issues jointly, and also together with quality, which is directly recommended by ISO 9000, 14000, 27000 and planned 31000 series.

Therefore, whenever speaking of:

- "business continuity" – it is spoken of postulated state of immunity of organization against disruption,
- "ensuring business continuity" – it is spoken of series of planned events, which aim at preventing disruption or removing causes and effects of disruptions, or introducing alternative conditions for activity until the effects of disruption are removed,
- "managing business continuity" – it is spoken of a management process, which consists in defining tasks, planning and monitoring the elaboration of solutions for ensuring continuity, evaluating actions and drawing conclusions from potential and existing disruptions, which aim at ensuring business continuity.

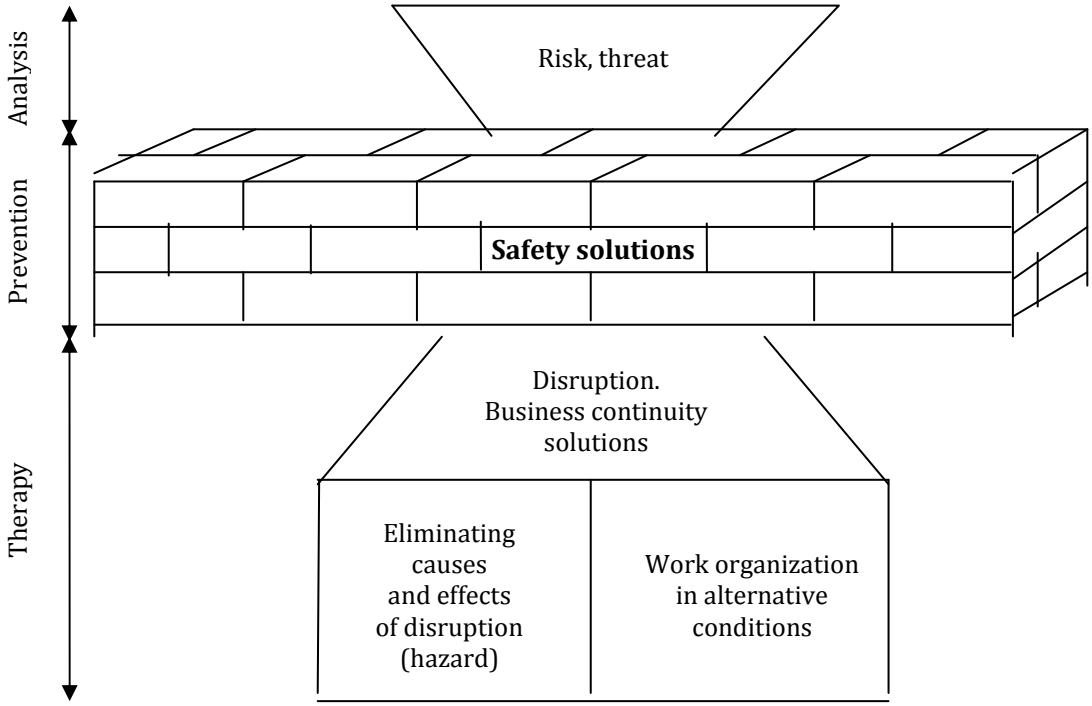

Figure 1. Relations between safety and business continuity ensuring tasks
(source: self study)

Organizational activity which aims at ensuring business continuity refers to the following issues, that should be taken into account or ensured:

- when a given threat influences the business system or its direct surrounding and the system becomes susceptible to this influence, we are dealing with a disruption, which:
  - is a result of an interaction between threat and business system or business system's surrounding,
  - results with considerable changes in the area of system functioning,
  - cannot be subject to objective evaluation, while subjective evaluation is made from the point of view of business system,
- possibility of occurrence of disruptions, which will obstruct normal continuation of the organization activity,
- independently from the character of reasons of these occurrences, as part of a formal or perceived in business categories responsibility to do one's best to execute their tasks, an organization should aim at least at limited continuation of business,
- this effort should be based on pre-elaborated, consistently perfected and tested plan for business continuity, sometimes also called (though in a slightly narrower sense) the emergency plan,
- ensuring business continuity means foreseeing scenarios of potential disruptions and separate design of:
  - solutions preventing the threats themselves (mainly ensuring safety),
  - solutions for quickest possible removal of effects of disruptions,
  - solutions for continuation of limited activity in critical conditions,
- attitude towards the problem of business continuity ought to be rational, that is, targeted at obtaining balance between expected level of certainty of maintaining business continuity and costs of reaching it; it is, therefore, necessary to adopt the assumption of gradual giving up of specific elements of normal business, adequately to the identified magnitude of the critical situation (persistent effort towards maintaining business continuity does not always have sense, especially from the point of view of economics),
- continuity plan should be elastic enough to enable adaptive reaction to disruptions which differ from the expectations, which were the base for the plan,
- it is necessary to define the core process of a given organization as a minimum set of actions, which still allows to conclude that the organization serves its purpose; inability to carry out such a minimum

set of actions is the basis for the decision concerning abandoning the use of continuity plan and concentration on removal of disruption effects only,

- when elaborating a continuity plan, business, legal and organizational issues are considered in the first place, as they determine the necessary scope of technical solutions,
- business analysis may cover the issue of company prestige and, surely, balancing risk as well as financial means devoted to its risk limitation; it is wise to treat the continuity plan as a long-term project, in which the marked out goals are achieved gradually, by means of consequent approximations (versions of business continuity plan),
- legal analysis is especially important when creating assumptions of continuity plan, because it enables to define the scope of company responsibility for particular fields of its activity, point out trouble spots and choose appropriate non-technical safety measures,
- organizational analysis enables to distinguish members of staff appropriate for using the continuity plan in critical conditions, to create an adequate level of decision autonomy in this situation and, in everyday conditions, enables to preparation for such a difficult role,
- none of the analysis elements, nor the design of technical solutions, is a self-contained stage; improving the continuity plan consists in constant repetition of analyses and design of solutions, which refer to changes in organization activity, development of continuity plan and conclusions from real disruptions.

In accordance with the ISO 27002 standard, when managing organization activity one should design solutions which effectively ensure maintaining business continuity of the organization. Analogically to living organisms, these solutions are to determine the ability of homeosthasis, that is, the characteristic of an organization which consists in launching own, inner mechanism of counteracting disruption in order to restore the situation from before this disruption. Effectiveness of disruption-anticipating solutions and their adequacy with reference to real occurrences should place itself above the minimal acceptance level of decision-makers. The decision-makers' evaluation is usually based on two criteria:

- organization prestige and the degree of its impairment in case of limiting or suspending activity,
- relation of costs of safety solutions to costs of potential losses and costs of resuming action that was disrupted.

Rationally viewed homeosthasis of a business system leads to conscious, temporary limitation of business quality, to the level pre-determined in the light of such determinants as:

- loss of an unsatisfied or harmed client,
- benchmarking with respect to competitors or best market practices (benchmarking is a systematic and continuous process of measurement; goal of the process of constant measurements and comparisons of organizational activity to leaders in economic processes worldwide, is to gather information, that will help the organization to undertake actions which will improve its functioning"; definition of American Productivity and Quality Center, B. Andersen, *Benchmarking*, 1992),
- reliable standards for cooperation with clients and partners, so called "service level agreement" (realistic and precise definition of parameters of provided services by the involved parties, including acceptable levels of unavailability of those services, as not violating the terms of a contract, i.e. servicing contract. See also: Hiles A. „Service Level Agreements: Measuring Cost and Quality in Service Relationships", Chapman & Hall, London, 1993).

Systematic approach to disruptions consist in determining:

- which disruptions (threats in interaction with business system) are being counteracted, that is, are covered by procedures for prevention or procedures for ensuring continuity,
- which technical infrastructure objects are protected against possible threats,
- which business processes are protected against threats,
- which information flows are being protected against threats,
- who is responsible for restoring business continuity in case of occurrence of disruption.

Limiting the quality of functions should not last longer than the amount of time needed to remove causes and effects of disruption, whereas the former can disappear by themselves if such is the nature of the disruption.

2 Organization of management

Ensuring business continuity, being an indissoluble organizational activity, needs to be permanently fixed into the organizational structure and formal documentation, which describes the structure, its rights and obligations (regulations, scope of obligations, procedures of activity). The term "permanent organizational activity" refers to the fact that business continuity tasks concern all the employees and all the organizational units and their managers, together with the current tasks, execution of which could be disrupted. In case of some professions it can also be pointed out, that ensuring continuity lays in their immanent nature (i.e. profession of engineer) both in the aspect of content matter (i.e. in design, the unreliability of technical solutions should be assumed) and ethics.

Subsequently, from the organizational point of view, it is necessary to distinguish between current efforts towards maintaining business continuity in the face of minor difficulties in task realization (at all posts and in all situations) and planning of reaction of bigger organizational parts or the whole organization to events, which are extensive accidents (catastrophes). The former one, in the model organization management, is written down in the organizational regulations, in the area of rights and obligations scope of organizational units, employees and management. Obviously, both categories should be, furthermore, divided into preventive actions towards probable disruptions and repair actions in case of occurrence of disruption (see Table 1).

Table 1. Classification of business continuity ensuring actions
(source: self study)

	Current	Emergency
Prevention	Technical checks Material inventories Servicing attendants	Emergency plans and ressources
Reaction	Help-desk Servicing	Alternative work organization in emergency conditions

The latter one, that is preparation for extensive accidents, requires special organizational solutions. Their main prerequisite is the character of events, for the occurrence of which one has to prepare, and, in particular, their possible extensiveness and possible far-going dissimilarity to the experience of current operations. This prerequisite justifies specific solutions, however, it is important to remember that the issues of ensuring business continuity are strictly related to ensuring safety in different aspects. The organizational solutions should, therefore, be created together and work simultaneously for the benefit of solving the both general problems.

These solutions may be divided into categories from the fields of:

- forming of the organizational structure,
- formal regulation of code of conduct,
- direct solutions for ensuring business continuity.

In the field of forming of organizational structure, the tasks of ensuring business continuity should be a part of a general concept of operational risk management. To high extent this depends on the given entity's specific character, including its size, because the smaller the entity, the more direct its management's involvement in solving each particular problem, managing risk, safety and business continuity is. The other way round, as we describe hereafter, looks the model solution concerning large companies, corporations in particular, where the highest management levels are in fact detached from operational practices and require support in the face of extraordinary events (including malfunctions), but also with regard to operational risk management.

Figure 2. depicts such a model example based on international recommendations of so called Basel Committee (full name is the Basel Committee on Banking Supervision, an international consulting body acting in the character of "wise men council", which operates in the banking sector next to the Bank for International Settlements in Basel, where the committee takes its popular name from, created for the purpose of establishing common recommendations of good practices. The result of the Committee's work is an extensive group of recommendations well known under the names of Basel I and Basel II. See www.bis.org/bcbs).

The highest management (boards) of these entities deals in practice almost exclusively with strategic matters, especially in the sense of long-run decisions, and from among the current problems only with large-scale ones. Current affairs management is handed over to a new level of high management (managing directors), created solely for this purpose, based on the new type of organizational structure orientated towards market-segments, client target groups, product and related processes.

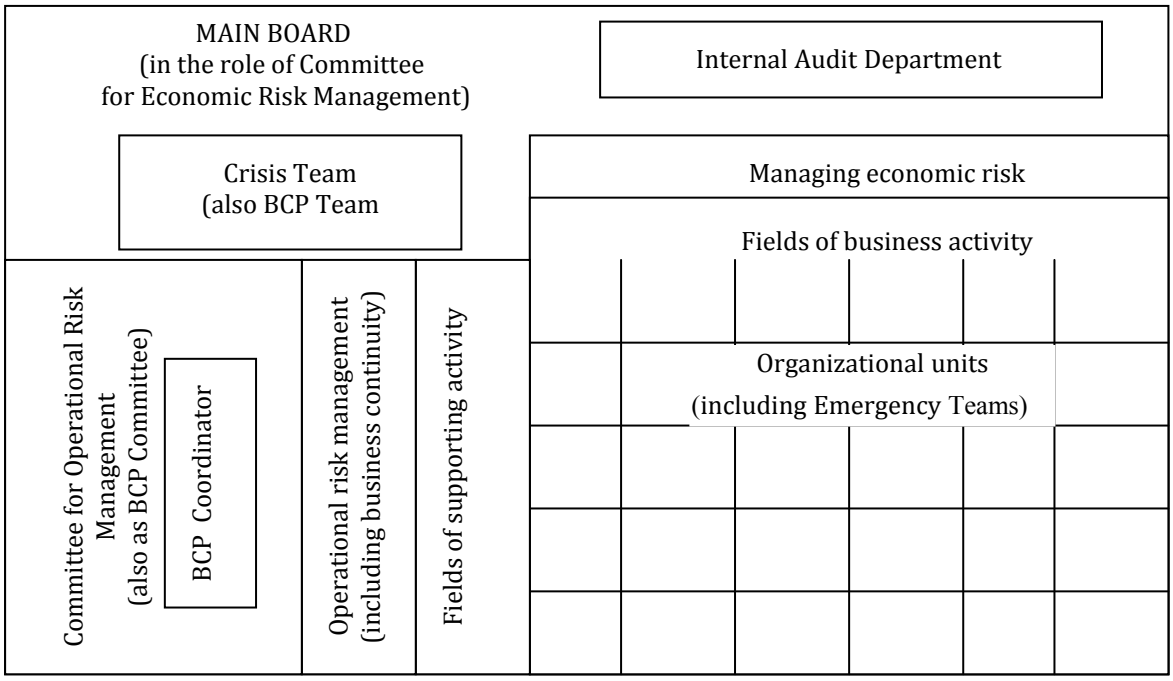

Figure 2. Model of risk, safety and business continuity management organizational structure, according to recommendations of the Basel Committee
(source: self study)

In banks, for example, separately managed departments of retail, institutional and investment etc. banking are established in accordance with the process approach. These departments become strongly autonomous parts of organization with their own strategy, plans and budgets as well as independent plan of supporting resources, which constitute material, technical and organizational basis for operating conditions, that is, realization of business plans. This basis consists of i.e.: workstations' equipment, ensuring staff with proper qualifications, IT services etc.

Taking into consideration the size of business and, simultaneously, the expectation of high effectiveness, not only organizational (quality, punctuality, productivity), but also cost-related, the particular parts of supporting activity require perfect organization and even greater effectiveness and, subsequently, resistance to disruptions, than core business activity. As a result, it is necessary to see the need for clear detachment of economic (business) risk management, such as: market, financial or legal risk etc, from operational risks (of internal organization).

From the above mentioned prerequisites results a concept of two decision centers which, in the documentation of Basel Committee, are referred to as Councils. One of them is business-tasks-oriented and devoted to managing economic risk, while the second one is supporting-actions oriented and manages operational risk (risk concerning appropriate organizational effectiveness in the field of realization of business activity supporting processes).

Let us notice that the Council/Committee for Operational Risk Management, recommended by the Basel Committee, is a task-orientated body, which proceeds periodically, possibly even regularly and often. After all, this situation is not very different qualitatively from the way the Board acts (as a kind of Council/Committee for Economic Risk). On a day to day basis the Board Members function in individual roles, determined and accounted for separately, and form the actual board only *en bloc* in situations described by the Commercial Companies Code and charter of the organization. Acting as a Board they make use of a certain office, team and control apparatus (i.e. board services office, team of advisors, internal audit department), directly subordinate to it. The case of Operational Risk Committee should look analogically.

At the same time, the current office work apparatus of the Operational Risk Committee can be dedicated to the matter of ensuring business continuity or analyzing

and preventing operational threats. In this work it was called BCP Coordinator. With regard to the fact that operational threats may materialize, there is a need to establish another task-oriented body such as Crisis Team (BCP team) apart from the existing permanent organizational structure. This team, in the time of peace and order, should systematically prepare itself and the whole organization for planned mobilization in case of critical disruption, malfunction and catastrophe.

With regard to ensuring business continuity, the fundamental roles depicted in Figure 2. are as follows:

- BCP Committee (alternately as a part of Committee for Operational Safety) – task-oriented body which gathers periodically it should have high level of authority coming from the Board (best solution is that it contains one Board Member); it is to delegate (and account for the execution) specific tasks to the individual organization units, as a part of gradual preparation of BCP documentation and solutions and acquiring skill of acting in crisis situations,
- BCP Team (or Crisis Team) – team of specialists, equipped with appropriate authorization of the Board and adequate means, prepared for directing crisis recovery process, should a crisis occur,
- BCP Coordinator – person or team of people who should possess the authorization of the BCP Committee (Operational Safety), in order to coordinate the realization of tasks set by the Committee for individual organization units in the periods between the Committee meetings; it is also responsible for running and distributing up-to-date BCP documentation (plans, scenarios), organizing trainings and tests; in case of a crisis it supports the BCP Team's actions,
- Emergency Teams - task-oriented bodies needed by individual local units, subordinate to the BCP Committee, acting locally in the same manner in which the BCP Team operates centrally; if needed, in case of a crisis, also in the main office (headquarters), task-oriented bodies in the most important cells, such as administration or IT departments.

3 Rules of Management

Problem of ensuring business continuity should be viewed in four categories of situations, which might occur in the light of basic risk factors, which are: probability of realization of a given critical incident and the size of potential result of this incident. This is illustrated in Figure 3.

Tolerance refers to acceptance of temporary inconveniences. Monitoring means that knowledge about the disruption is sufficient for launching of a compensation mechanism. Prevention means actions towards aversion of negative effects of disruption. Business Continuity Plan is a set of scenarios describing expected realization of threats and planned responses to these threats.

Approach of Tolerance should be connected with those disruptions, which in their nature are external to the organization, and secondarily relate to the organization; especially those which are non-invasive and not destructive. For example: Transportation company which distributes press – waits through the morning fog and distributes the newspapers later.

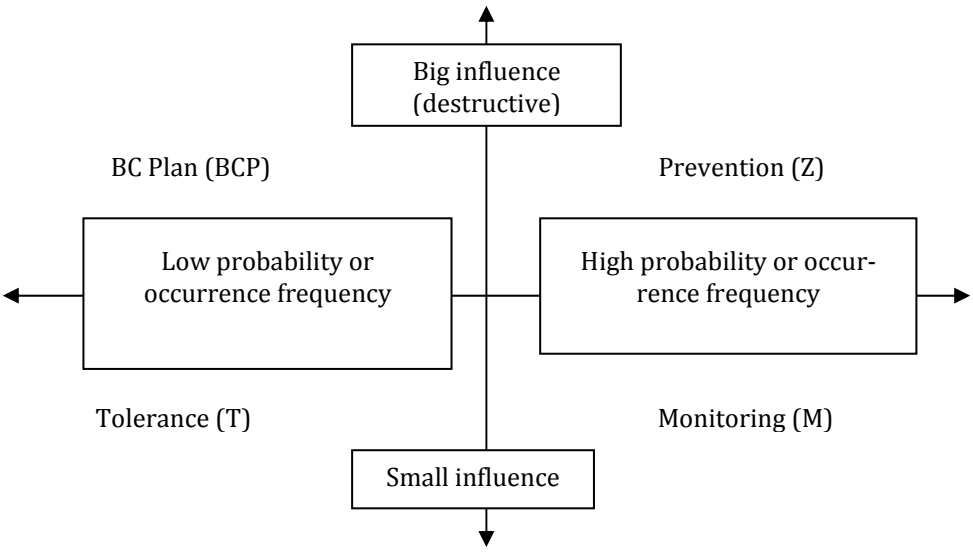

Figure 3. Model approach to disruptions
(source: self study)

Monitoring approach should be connected with dealing with those disruptions, which in their nature are small but frequent (therefore, their incidentally bigger influence as a result of accumulation in short period should be assumed), however, clearly not destructive. This strategy should result in a detailed solution through organizational actions and detailed internal regulation of reaction to all typical disruptions. The essence of this strategy is a faint or none rise in costs resulting from reaction solutions, as they have, above all, organizational character. For example: employees' sick leaves – obligation to inform the company beforehand and established rules for organizing replacements.

Prevention approach should relate to substantial, destructive and potentially frequent disruptions. The natural consequences of the prevention strategy are investments and solutions which limit the risk of threat. Typical action is creating back-ups of technical solutions. For example: frequent energy shutdowns – installation of uninterruptible power supply or power generators.

Business Continuity Plan approach should be connected with reacting to substantial, destructive but potentially rare disruptions, which supports the decision about resigning from Prevention approach and conscious acceptance of the related risk of threats. For example: Stock exchange – world statistics say that stock quotations are suspended because of computer system malfunction no more often than once every three years and the suspension does not last longer than one day. It is, therefore, reasonable to rely on an alternate functioning scenario in case of such a rare but serious malfunction.

Policy of Tolerance (T) should specify the basic conditions which must be met for a company to approach to accept the disruption which occurred, research the prerequisites for its duration, affirm its regression and return to the routine functioning. T Policy documentation should encompass procedures/instructions describing in detail the necessary actions of organization cells in case of disruption which qualifies to be subject to this policy. For example: although the organizational reaction for disruption may, at the end, consist in suspending the execution of statutory functions, maybe it is necessary to communicate this fact to trade partners and to the public, reallocate workers to substitute duties which are unaffected by the disruption, launch solutions which track the intensity level of the disruption. In the moment the disruption disappears, it has to be verified whether it is possible to restore the previously suspended activities/functions.

Policy of Monitoring (M) should specify the basic rules of organizational reaction to disruptions, with regard to which the awareness of their occurrence together with the existing regulations (if need be, written down as procedures and instructions) should, to the sufficient degree, launch the organizational mechanisms of disruption compensation. M Policy documentation should encompass procedures/instructions describing in detail the necessary actions of organization cells in case of disruption which qualifies to be subject to this policy. For example: in a bank, it is obligatory for the direct client service personnel to inform beforehand about the absence caused i.e.: by illness; defined number of back-office personnel members are trained to be able to work as replacements in case of an extraordinary absence, that was not communicated beforehand by a front-office worker.

Policy of Prevention (P) should specify the organization plans concerning preventive actions, which ought to neutralize the destructive influence of disruptions with regard to particularly important elements of organizational activity, especially the sensitive elements of its technical infrastructure. P Policy documentation should contain detailed analyses of the degree and scope of sensitivity of existing solutions, plans of solutions which could decrease the threats, procedures/instructions describing in detail the organization and rules of current operations as well as specialist teams interventions aimed at fighting specific threats (fire, hacker attack, IT malfunction). For example: back-up computer center, multiple means of communication, using different physical paths and transmitting media. Also, keeping special intervention groups with appropriate qualifications on duty.

At the same time, it is important to underline that each object-threat couple contained in policy P, the preventive actions plan, if it consists in threat-decreasing investment, should be, simultaneously, included in one of the other policies until it is finished, in order to ensure proper reaction to threat (it is recommended to include it in BCP policy).

Policy of Business Continuity Plan (BCP) should specify the organization plans concerning actions which are necessary in case of realization of a threat. Plans should encompass organization plans with regard to carrying out the Policy itself and different case scenarios

of disruptions and planned counteractions, aiming at ensuring continuity of at least core business of the organization. Moreover, BCP policy should define the rules of ad hoc reactions to events which, unfortunately, could not be foreseen in the scenarios (at all or with regard to scale). BCP policy documentation should contain procedures/instructions specifying in detail the organization of bodies which carry out the business continuity plans, basic rules of communication in face of emergency, rules of reaction to typical threats, scenarios of expected extensive disruptions and reacting to them, rules for including the experiences from current disruptions in the future versions of emergency plans.

Managing business continuity is such a young area of knowledge, that it is hard to find a commonly used and well practice-based methods of its evaluation. Nevertheless, such proposals have already appeared. The most famous one is the Business Continuity Maturity Model (BCMM), a method established by an American company Virtual Corporation Inc., www.virtual-corp.net, see Table 2.).

Idea of the method is such that a company (an organization) gradually reaches higher levels of maturity by introducing permanent organizational structures, participants' roles, rules and action plans. Simultaneously, it is possible to step back in situations when the organization or its surrounding undergo profound technological or organizational changes. Particular levels are characterized as follows:

- Level 1

The highest management does not think that BCP problems are important or require being centrally governed. BC issues are dealt with by individual organizational cells according to their own level of expertise and to the level they consider right.

- Level 2

Strategic meaning of BCP problems is recognized by some organizational unit. In the organization or among its specialist advisors there is a specialist, who can support BCP works. The highest management views BCP as an important matter, but does not prioritize it properly yet. Level 3 – Organizational cells which are most interested in BCP problems carry out joint activities concerning BCP. However, it is not a BCP for the whole company. The highest management is aware of this initiative and actions, supports them, but is not able to establish proper structures, tasks and Business Continuity Plan.

- Level 4

The highest management is aware of the strategic meaning of BCP. Permanent office which deals with BCP problems is established. Integrated solutions for the company as a whole are being established. Critical processes were identified and protection plans were established. They are being tested and updated on a routine basis.

Table 2. Business Continuity Maturity Evaluation method
(source: Virtual Corporation, Inc.)

Maturity level of continuity management		Program Basics			Program Development		
		Senior-Management Commitment	Professional Support	Governance	All Units Participating	Integrated Planning	Cross-functional
Level 1	Self-Governed	No	**No**	No	No	No	No
Level 2	Supported Self-Governed	Marginal	Partial	No	No	No	No
Level 3	Centrally Governed	Partial	Yes	Partial	No	No	No
Level 4	Enterprise Awakening	Yes	Yes	Yes	Yes	No	No
Level 5	Planned Growth	Yes	Yes	Yes	Yes	Yes	No
Level 6	Synergistic	Yes	Yes	Yes	Yes	Yes	Yes

direction of maturity level growth

- Level 5

All organizational cells have tested BCP plans positively, including rules of introducing changes to plans. The highest management has also participated in the tests. Couple-year long BCP solutions development program has been elaborated.

- Level 6

All organizational cells have received high evaluation notes of BCP preparation. Cooperation of cells is tested. All factual changes in business processes as well as potential changes to BCP plans themselves are being followed and adapted to BCP solutions.

4 Designing and maintaining business continuity plans

The basis for implementation of policy of dealing with disruptions is a proper plan containing the following stages.

4.1 Analysis of organizational processes

Modern system approach to management is characterized by the concept of viewing organization as a business system, in which the key element is right and effective management of processes and not the classic functional organizational structure. Traditional views on organization described by the problem of effectiveness of particular functional departments and organizational cells lead to atomization of those organizational units, and the care for own, inner effectiveness, paradoxically, does not increase but decreases the effectiveness of the whole organization. What is more, striving for inner micro-perfection of organizational cells separates them from the environment, including, what is particularly critical, clients, cooperators and competition.

Process approach, on the other hand, leaving the improvement of functioning within the competence of organizational cells, means that management is concentrated on coordination of organizational cells' tasks and relations with the environment, in the light of clearly defined goals: organization, processes and workstations. Achieved in this way are:

- optimization of organizational functioning,
- rationality of organizational cells' cooperation,
- viewing client needs as the highest goal of an organization,
- viewing services as a result of relations with the environment,
- identification of the way work is performed.

Ant the work itself is viewed and organized through a process, that is, series of actions, as a result of which product or service is created. Process is also a chain of adding value. Identification and analysis of processes, as a starting point for decisions with regard to business continuity management, may result in drawing vital conclusions leading to reengineering of processes and work organization.

The result of process analysis is a so called "process map". For a single process, such a map is a sequence of operations, which lead to turning certain resources into effects. Creating a process map starts with identifying all the subjects (organizational cells) which participate in the process and, next, consists in describing which following actions, with the use of what resources, performed by which organizational cells, constitute the process.

Under the current, common use of IT solutions it is necessary to remember, that properly designed IT systems reflect the flow of processes through workstations, which are operated by a given system.

Table 3. Variables of Process effectiveness analysis
(source: [12], p. 61-109)

Organizational level	Organizational goals	Organization design	Organization management
Process level	Process goals	Process design	Process management
Workstation level	Workstation goals	Workstation design	Workstation management

Therefore, system analysis should accompany process analysis in order to:

- identify processes or their elements, if classic process analysis is impeded,
- verify if information/IT system properly and sufficiently operates the analyzed processes,
- identify physical paths of information flow, which supply, accompany (are the elements of) or are the results of a process.

The last point refers to determining places and paths for information flow, which may be threatened by the influence of disruptive factors.

Need for analysis of information and IT systems also results from the specific role of information in management, which, as a factor that increases our knowledge of the surrounding reality, is sometimes called the "blood-system of management". Information are the basis (input) for process management, describe the course of processes, are one of process inputs and results.

Information flows take place through physical paths (channels): traditional ones, which are defined by process organization or determined by telecommunications infrastructure. Potentially, this leads to physical discrepancy between paths of sharing information in an IT system (in this case, information sharing uses such technical channels of communication as: cable network, wireless network) in relation to traditional information flow consistent with process flow, viewed as relation between the following workstations. This discrepancy is an important factor which increases the critical susceptibility to disruptions.

Possible channels of information flow are:

- traditional, connected with passing paper documents,
- conventional telecommunications (phone calls, faxes),
- electronic telecommunications, providing digital data transmission.

When analyzing information flows, with regard to all the channels, we take into consideration:

- consistence and discreteness of information flow within a given business process,
- degree to which information flow accompanies business process,
- means of sharing information and their susceptibility to disruptions,
- degree to which basic means can be replaced by alternative ones,
- critical elements of information flow.

4.2 Analysis of threats to organization

Analysis of threats is made with the use of a model "list of threats" (see Table 4.). At the beginning the threats which are inadequate to the situation of a given organization have to be crossed out from the table and, possibly, other organization-specific threats need to be added.

Next, it is evaluated if a given threat has got internal or external character from the point of view of the organization. It has to be determined if the threat within the organization realizes itself in its real form and if it constitutes the organization's problem, i.e.: whether a hurricane is a properly identified threat, or should it rather be the damaged building structure. External threats result in internal ones and, therefore, we aim at determining the latter ones. Consecutive iterations of evaluation (verifications) may be needed in order to cross out the external threats as being unlikely or replacing them with more precisely defined external threats. Primary list of threats (including external threats) should be included in the safety policy in order to cover them with monitoring and preventive actions (i.e. we monitor the hurricane to secure the building).

In the next step, it is evaluated if a threat has a direct or indirect character. The case is, if the disruption in its essence relates to the organization, or it is a derivative factor that does, i.e.: if a demonstration is a disruption, or is it de facto the lack of access to the headquarters caused by the demonstration. Also in this case, the primary list of threats requires us to monitor and prevent, as a part of safety policy.

At the end, a final, verified list of threats is prepared, qualifying threats to be attended to within the safety policy and/or business continuity plan.

4.3 Analysis of disruption susceptibility of organization

This analysis is run with the use of "list of trouble spots" (see Table 5). First of all, the classification of objects' categories has to be verified and specified in an appropriate way with regard to organization-specific situation.

Table 4. Model list of threats
(source: self study)

Groups / Threats
Natural disasters - earthquake - environmental contamination - flood - hurricane - lightening
Terrorism - blackmail - attack
Disruptions to physical working environment - lack of access to headquarters - building defect - too low / to high air temperature - to high air humidity - fire - flooding
Disruptions to functional working environment - strike - sabotage - employee unavailability - accident
Disruptions to technical working environment - lack of resources - Lack of power supply - A/C malfunction
Disruption to IT working environment - technical infrastructure/hardware: ▫ servers ▫ workstations ▫ supporting devices ▫ network devices ▫ cable system ▫ lack of connection to external networks - software: ▫ license expiration ▫ unauthorized deletion ▫ faulty functioning - viruses - data: ▫ loss or damage of data ▫ unauthorized access to data ▫ unauthorized copying of data ▫ unauthorized modification of data

Next, all the objects which may influence the continuity of business and information flow processes, in the light of processes and information flow channels, have to be identified for each location of organizational unit (headquarters + local and supporting locations). Some external services which have particularly high influence on the organizational functioning conditions have to be taken into consideration as objects, including universal ones such as: water, gas, electricity, telecommunications, as well as specific ones such as: cooperation, supply of resources or servicing. As a result of the analysis, separate, verified lists of trouble spots are prepared for each location.

4.4 Map of disruptions preparation

At this stage, map of disruptions for physical places as well as technical and logical objects, which could potentially be influenced by particular threats (Table: process – object – threat) is prepared. Owing to this process, the final verification of threats is possible. This verification reveals which threats could be most severe and which objects are most business-sensitive. Criticality should be evaluated and verified from the point of view of maintaining process stability.

This is the most extensive analytical document. However, if prepared carefully, it enables to introduce complex solutions for ensuring business continuity. It should not be feared, that this document will lead to as extensive scenarios and detailed policy for ensuring business continuity. In reality, the specific and not numerous scenarios and plans, which constitute the policy, will refer to many elements of map of disruptions simultaneously and cumulate into just a few general scenarios. Specific parts of the map of disruptions are connected with appropriate model approach to disruptions, consisting in one of the possibilities: T (tolerance of disruption), M (monitoring of disruption), P (preventing disruption), BCP (business continuity plan), which are described later.

4.5 Elaboration of regulations, procedures and instructions

We speak of a complex set of action procedures and instructions when there exists a norm which enables preparing them in such a way, that they will encompass each area of company activity and that the way they are formulated will be homogenous. Such a norm is constituted by regulations.

Table 5. Model list of trouble spots
(source: self study)

Category	Example
Structures	Own office building
Industrial, technical objects	factory, boiler station, computer room
Office centers	Rented office space
External technical equipment	External standalone power generator
Internal technical equipment	Indoor A/C or generator
IT infrastructure	IT hardware
External telecommunication devices	Satellite antenna on the roof
External services	Telecommunications
Logical objects of virtual objects/solutions	Intangible commitments

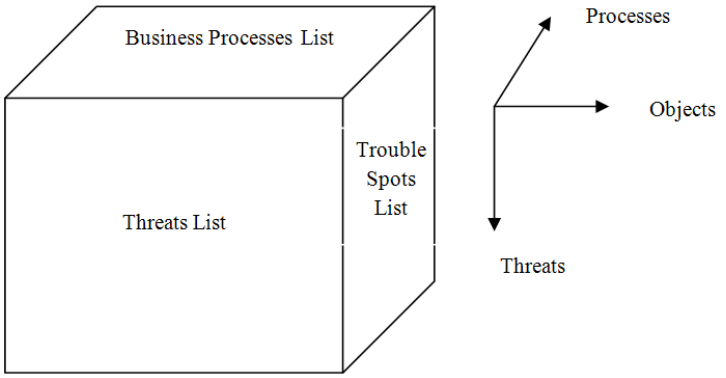

Figure 4. Map of disruptions
(source: self study)

Procedures are most often a written-down form of certain practice which is used and commonly viewed as appropriate. Only freshly established procedures are a record of bylaws. Procedures which exist some time and are verified appropriately often already encompass the experience factor and reflect real practices.

Complex set of procedures consists of different categories of documents, which regulate rules of actions and describe these actions. Procedures define the scope of rights, responsibilities, proper order of activities and bilateral relations between people and cells, which were entrusted with given fields of company activity. Instructions, on the other hand, are the documents which describe specific action steps of people and organizational cells.

In order to ensure completeness and coherence of procedures, both within one document and with regard to the complex set, a logical process for edition, verification and acceptance of procedures/instructions is required. The best way to ensure that is to create a separate procedure/instruction, which defines model of such process and model structure of specific documents. Complex set of action procedures becomes, gradually, an inner norm of appropriate action and, at the same time, a basic point of reference for organizational audit.

Typical categories of documents, which constitute a complex set of bylaws, procedures and instructions are:

- bylaws,
- general procedures which refer to the whole organization,
- inter-department procedures which regulate cooperation and competences of two or more organizational cells,
- department procedures which encompass tasks delegated to a given organizational cells,
- instructions which describe actions regulated by procedures,
- self-contained instructions, which do not refer to any procedures.

Category division implies an appropriate process of establishing, verifying and accepting procedures and sets the proper organizational level for accepting them.

Covering all organizational activities with a complex set of procedures consists in determining problem matters, processes and sub-areas that need to be analyzed and regulated. This is made by choosing basic criteria of distinguishing problem matters and, possibly, superposition of some criteria. Typical criteria and divisions are:

- organizational structure,
- sub-systems of IT system,
- business continuity, safety, correct exploitation.

It is important to adopt a homogenous formatting of common procedures and to include in them all the information which identify the procedure (symbols), its history, processes of establishment, evaluation and acceptance.

Each procedure should have its owner, that is, a cell/post responsible for editing, directing, evaluating and distributing it after it is introduced. Usually, the appointed owner is the cell which actions are most similar to those regulated by the procedure or a central cell responsible for a set of procedures.

It is necessary to run an archive of all consecutive versions of each and every procedure. Such a need results, among others, from audit requirements, that should be able to refer each doubtful situation (problem) from the past to the norm which was in force at the time.

4.6 Realization of disruption tolerance approach

This approach encompasses those actions which have legal character but also those of organizational character. In general, there is no substantial reaction to disruption. Nevertheless, it is necessary to regulate a number of issues of two kinds.

First of all, it is necessary to determine in which way the disruption intensity is measured and who, in what way, on what basis, decides about launching actions, that are planned organizational reaction to disruption. Analogically, this person decides about ending this activity and returning to routine execution of tasks. Organizational activity, which in its nature means tolerating the disruption, consists in stopping routine work and may require informing all employees, clients, co-operators, etc. about it. This should be predicted within appropriate situation scenario.

Secondly, it is important that business responsibility towards partners (clients, employees and service-providers) is defined and limited adequately to the formulated policy.

It may consist in:

- placing contractual clauses defining the influence of "higher power" on the business responsibility for provided services,
- standardizing conditions of providing services (service level agreement), defining the acceptable level of service inaccessibility (e.g. 1 hour per year) or acceptable substitute solutions,
- clear definition of limitations of company solutions and responsibility for them (e.g. only until the communications centre of a public network),
- reserving the right to monitor or even intervene in partners' solutions,
- grading scope, quality and price of services and their automatic limitation in case of disruption.

4.7 Realization of disruption monitoring approach

This approach encompasses, above all, organizational actions and, secondly, regulatory actions. Of key importance is the monitoring of disruption level and the fact if mechanism of routine compensation is satisfactory here. Establishing solutions of this policy consists in formal confirmation of organizational solutions concerning compensation of disruptions. Subsequently, it requires writing down, analyzing and, possibly, correcting or developing the existing practice as well as taking into consideration which solutions are necessary in the field of organizational structure design, tasks of particular cells, bylaws, procedures and instructions.

Table 6. Typical minor disruptions and their compensation *(source: self study)*

Disruption	Compensation
- absence - unpunctual supplies - relative/ unclear decisions - equipment malfunction - overloading - limited productivity/ capacity	- replacements - inventories - written orders/ confirmations - servicing attendants - repetition - delays

The mentioned monitoring of disruptions should be regulated by procedures/instructions in such a way, that it is possible to evaluate and make decisions in situations when degree of disruption exceeds the limits of monitoring policy and should be confronted with the business continuity plan approach.

4.8 Realization of disruption prevention approach

This approach encompasses, above all, investment activities, but also, until the investment is realized, business continuity plan approach activities. The map of disruptions implies certain number of weaknesses of an organization (in the sense of business continuity problems). Most of these weaknesses may be limited or eliminated through investment in technical equipment. Typical investment directions are:

- doubling equipment,
- building back-up computer centers,
- multiplying the number of communication lines,
- multiplying access points to public services network,
- emergency sources of electricity,
- physical, energetic and logical separation of servers and IT centers,
- despite of specialization of servers, keeping the possibility of limiting the number of them being used,
- asynchronous process of securing data,
- specialists on duty.

An investment plan, accepted by the decision-makers responsible for technical solutions, is the fundamental document, on which the activities of this approach are based.

4.9 Realization of business continuity plan (approach)

It encompasses activities understood strictly in accordance with intuitive apprehension of goal and scope of ensuring business continuity. These activities are divided as follows:

The essence of business continuity plans are the situation scenarios. They are divided into:

- external scenarios, which describe possible versions of future development of events, on which the organization has no influence,
- internal scenarios, which reflect causal way of reasoning, that connects choice of action and the goal. Particular results are preferred by the organization in accordance with its hierarchy of goals (van der Heijden K., "Scenario Planning in Strategic Management").

Table 7. Task divisi on in reacting to disruptions *(source: self study)*

Organizational cell	Before occurence of disruption	After occurence of disruption
Permanent Anti-Crisis Team	Establishing business continuity plan	Analysis and improvement of business continuity plan
Crisis Team	Testing of business continuity plan	Ensuring business continuity, removing causes and effects of disruption

When working on scenarios, especially during first approach to create the business continuity plan, a very fundamental "top-down" way of thinking, which reaches to knowledge about organization and its goals, has to be adopted (traditional name for practice of describing, analyzing and solving problems). Consecutive steps of such reasoning (some of which can be omitted) are:

- establishing goals (even organizational mission),
- establishing the core organizational activities (core processes) on the basis of process analysis,
- establishing acceptable limitations to concessions in case of disruption (with regard to scope of necessary activities and minimum, yet accepted, quality of activity),
- evaluation of threats and disruptions which result from them (verification of disruption map),
- evaluation of current ability of organization to *ad hoc* react to disruptions,
- introduction of organizational solutions aimed at facing disruptions (appointing BCP Coordinator and Crisis Team and establishing proper bylaws, rights and obligations),
- establishing scenarios of disruptions and ways of counteracting them,
- testing of situations described in scenarios,
- verification of the above mentioned procedure on the basis of tests and conclusions drawn from the occurrence of disruption.

Model of situation scenario is shown in Figure 5. Situation scenarios:

- put our expectations in order,
- mobilize to concrete, precise reasoning and acting,
- enable simulation of critical situations and testing of elaborated plans.

Simultaneously, it is important to remember that scenarios:

- do not guarantee complete accuracy of expectations with regard to disruption, course of action of critical situations, adequacy of plans to real events,
- require leaving a flexible margin for unpredicted factors/events.

4.10 Dealing with disruptions

Implementation of policy of dealing with disruptions consists of three streams of activity:

- creating formal organizational structures,
- defining rules of monitoring threats and reacting to disruptions, investment plans and models of emergency scenarios,
- establishing bylaws, procedures and instructions, as well as detailed action scenarios in case of disruption.

Two aspects have to be considered with regard to organizational structures dedicated to business continuity management. First of all, the already signalized division into permanent, current execution of activities such as preparation and administration of business continuity ensuring policy (so called BCP Coordinator) and activation of Crisis Team. Secondly, experiences of risk management theory and good practices worked out in some industries, such as banking, have to be taken into account. In this context, disruptions to business continuity may be viewed, partially, as realization of business risk and, above all, operational risk.

Such approach leads to viewing the issue of ensuring business continuity as an element of operational management referred, above all, to supporting cells' activity, which ensures business cells the necessary technical, organizational, logistic and formal conditions of functioning.

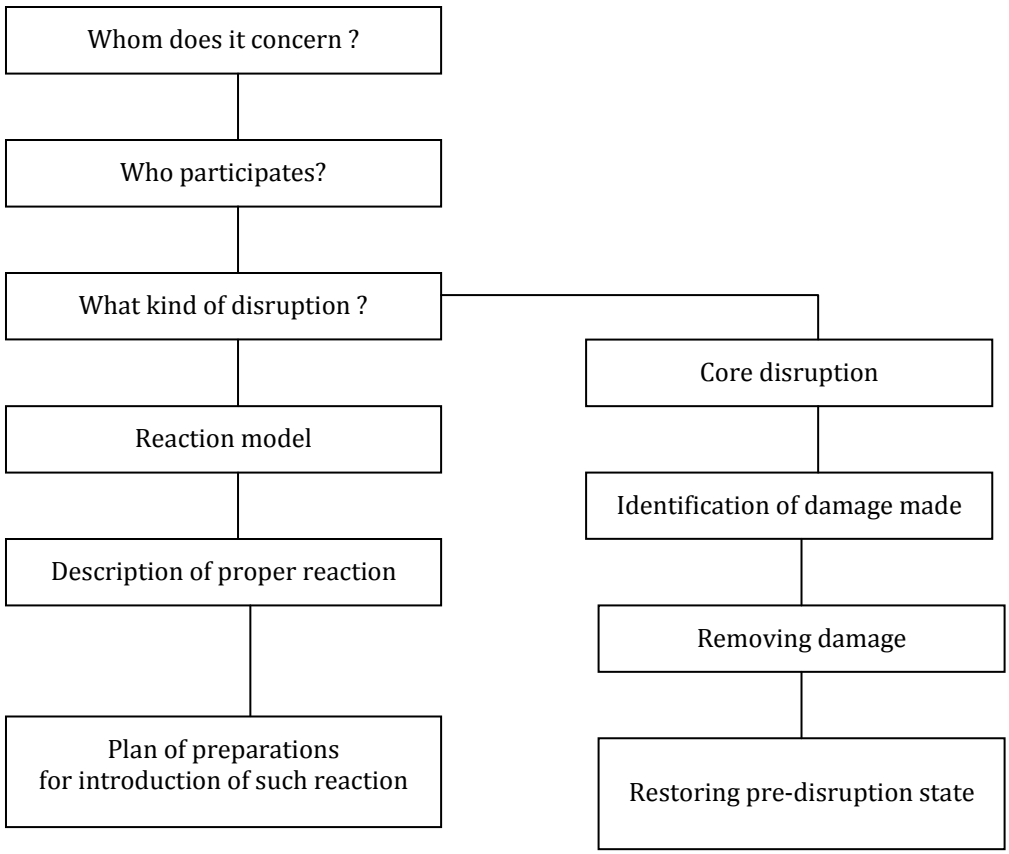

Figure 5. Scheme of situation scenario of reaction to disruption
(source: self study)

Implementation of policy for dealing with disruptions should be based on a few rules which are characterized below. First of all, it is important to aim at completely aware management of business continuity problems, through:

- identification of the core of organization activity,
- determining the hierarchy of importance of functions and processes,
- evaluation of determinants of ensuring business continuity including the cost factor,
- determining the acceptable limitations to concessions with regard to efficiency and quality of activity.

Secondly, in search of the right solutions, it is important to appreciate non-engineering means, because:

- technical solutions are complicated, most expensive but never completely effective,
- instead of technical solutions, it is more wise to search for legal and organizational ones.

Thirdly, it is very important to care for adequacy of solutions to real, current possibilities of the organization, as:

- already the execution of current activities uses, in fact, almost maximum capacity of organization,
- in face of disruption it is better to simplify the problem,
- in face of disruption it is better to limit the activity reasonably and according to a plan.

Fourthly, with regard to the above mentioned rules, solution simplicity should be pursued, because:

- each new solution brings about new threats,
- new solutions, especially technical ones, are also fallible,
- there always exists a threat of not being able to carry out a complicated solution.

Fifthly, intellectual power contained in human inventiveness should be appreciated. In order to do so, one must remember that:

- outstanding experts are reliable when it comes to extraordinary solutions, especially when disruption varies from the planned scenarios,
- person becomes a specialist through cumulating experiences and due to trainings,
- problems often appear on the touching edge of two specialties, and require knowledge of them,
- apart from specialists from within the organization, external consultants may be useful.

In implementation, it is important to remember that specific solutions of policy for dealing with disruptions should be introduced both for the whole organization and for its local branches. Simultaneously, one must consider looking at particular planned events and actions as well as documentation, which describes them, both from the perspective of the whole organization and from the perspective of individual organizational cells, identified as involved in given problem in the course of business processes' analysis. Planned scenarios of events and disruptions should also include variants depending on the time of disruption occurrence. Last but not least, one should not forget about the issue of restoring the situation from before the disruption.

4.11 Testing of business continuity plans

Situation scenarios are a proper basis for testing organizational readiness for facing the disruptions. Disruptions can be, for the sole purpose of tests, appropriately simulated or even deliberately induced.

Tests are an element of improving business continuity solutions and, therefore, should be planned regularly and as often as possible. First of all, they serve the purpose of checking solutions themselves, their adequacy to the situation, completeness, sufficiency of owned resources, reserves and qualifications. Secondly, they are used to train employees and organizational cells in applying planned scenarios and using emergency solutions.

Nevertheless, one must be very careful when running tests in real-life conditions and carry them out only after obtaining positive results of departmental and partial tests. In face of doubt concerning quality of preparations to tests or plan of test, it is better to postpone the test than to risk losing control over the situation.

When testing, one should gradually move from:

- partial tests to complex tests,
- tests in artificial conditions to tests in real-life conditions,
- tests in times when work is not performed to tests during normal work,
- tests including only chosen employees to tests including all employees.

It is extremely important to remember about testing the return from alternative work organization caused by

disruption to work organization from before its occurrence.

4.12 Constant improvement

One fundament of organizational culture is not to finish with currently elaborated and implemented solutions, but to constantly consider them imperfect and work on their improvement and development. It is also clearly stated rule included in the new generation of quality standards (See PN-ISO-9001:2000). It refers solely to business continuity management.

When following such approach, it is necessary to appoint a Permanent Anti-Crisis Team, the most general task of which is to elaborate and constantly improve the solutions devoted to ensuring business continuity. Simultaneously, a direct, substantive improvement of solutions is required, based on testing and careful analysis of their adequacy to actual disruptions of business continuity.

The space for improvement is considerable, which results from realistic design of solutions, both with regard to rational limits of concessions in face of an aggressive disruption and modest, defensive evaluation of own capabilities of reacting to disruptions. In general, the more modest the expectations towards the scope of business continuity ensuring solutions' effects, the higher the effectiveness of implementation of primary versions of solutions, but also, the bigger the area for gradual improvement.

A number of improvement techniques are devoted to this idea (Dahlgaard J.J., Kristensen K., Gopal K.K. „Fundamentals of Total Quality Management", pp. 59-67.) in the sense of analysis of causes of insufficient quality and determining ways of reaching better solutions. Basis for this improvement are people, their knowledge and involvement, which can me shaped, and effective organization, which can be established and developed.

5 Summary

First of all, business continuity is a postulate of business system perfection, where business system refers to each and every organization, thus to all economic or administrative entities. In this sense, ensuring business continuity is the subject of strategic management, putting forward the primary goal of organizational efficiency and taking over the field of operational risk management.

Secondly, business continuity is viewed as such organization behavior which creates the ability of an organization to effectively react to disruption as a result of a specific interaction between signs of threat and inner organization's vulnerability, infrastructure or resources. In this sense, ensuring business continuity is the subject of operational management and is the last cell of operational risk management.

In general, business continuity is the ability of an organization to react to disruptions in normal business conditions in such a way to, where it is possible, restore those normal conditions and, where it is not, to switch to a planned method of alternate execution of actions. Therefore, business continuity is viewed both in the context of organization tasks and processes for realization of these tasks, as well as in the context of factors which may disturb those processes and organization vulnerabilities, which determine its disruption sensitivity.

6 References

[1] Andersen B. - *Benchmarking* [in] Performance Management (ed. A. Rolstadas). Chapman & Hall, London 1995.

[2] Antoszkiewicz J.D. - *Firma wobec zagrożeń. Identyfikacja zagrożeń*. Poltext, Warszawa 1998.

[3] Augustyn S. - *Praca menedżera programów kryzysowych na lokalnych szczeblach zarządzania* [in] Samorząd terenowy wobec nadzwyczajnych zagrożeń. Bydgoszcz 1998.

[4] Dahlgaard J.J., Kristensen K., Gopal K.K. - *Podstawy zarządzania jakością*. PWN, Warszawa 2000.

[5] Dworzecki Z. - *Skuteczne zarządzanie w sytuacjach kryzysu*. TNOiK, Warszawa 1993.

[6] *Guide to Business Continuity Management*. British Standards Institution, 2003.

[7] Heath R.L. - *Crisis Management for Managers and Executives*. Financial Times Pitman Publishing, London – San Francisco 1998.

[8] van der Heijden K. - *Planowanie scenariuszowe w zarządzaniu strategicznym*. Oficyna Ekonomiczna, Kraków 2000.

[9] Hiles A. - *Service Level Agreements: Measuring Cost and Quality in Service Relationships*. Chapman & Hall, London 1993.

[10] Hiles A., Bearnes P. - *The Definitive Handbook of Business Continuity Management*. John Wiley & Sons Ltd, Baffins Lane - Chichester 1999.

[11] Mitroff I.I., Pearson C.M. - *Zarządzanie sytuacją kryzysową*. Business Press, Warszawa 1998.

[12] Rummler G.A., Brache A.P. - *Podnoszenie efektywności organizacji*. PWE, Warszawa 2000.

[13] Tyrała P. - *Zarządzanie kryzysowe*. Wydawnictwo Adam Marszałek, Toruń 2001.

[14] Zawiła-Niedźwiecki J. - *Metoda TSM-BCP - Total Security Management, Business Continuity Planning*. European Network Security Institute, Warszawa 2003.

[15] Zawiła-Niedźwiecki J. - *Propozycja metodyki zarządzania ciągłością działania* [in] Przegląd Organizacji, No. 6, 2003.

[16] Zawiła-Niedźwiecki J. - *Ciągłość działania a teoria zarządzania* [in] Ekonomika i Organizacja Przedsiębiorstwa, No. 4, 2006.

[17] Zawiła-Niedźwiecki J. - *Problem dobrych praktyk zarządzania ciągłością działania w instytucjach finansowych* [in] Komputerowo zintegrowane zarządzanie(ed. R. Knosala). Wydawnictwo Politechniki Opolskiej, Opole 2007.

[18] Zawiła-Niedźwiecki J. - *Model oceniania dojrzałości zarządzania ciągłością działania organizacji* [in] Przegląd Organizacji, No. 4, 2007.

[19] Zawiła-Niedźwiecki J. - *Dobre praktyki czy teoria zapewniania ciągłości działania* [at] Ogólnopolska Konferencja Naukowa nt. Zarządzanie rozwojem organizacji, Politechnika Łódzka Katedra Zarządzania, Spała 10-12.05.2007.

[20] Zawiła-Niedźwiecki J. - *Projektowanie rozwiązań zapewniania ciągłości działania* [at] Konferencja Management Forum 2020 nt. Współczesne i perspektywiczne kierunki badań w zarządzaniu przedsiębiorstwem, Akademia Ekonomiczna w Katowicach, Ustroń 9-10.05.2007.

[21] Zawiła-Niedźwiecki J. - *Business Continuity Management, from best practices to maturity model* [at] 11th International Conference on Human Aspects of Advances Manufacturing: Agility and Hybrid Automation, University of Louisville + International Ergonomics Association + Politechnika Poznańska, Poznań + San Diego 9-12.07.2007.

[22] Zawiła-Niedźwiecki J. - *Rozwiązania bezpieczeństwa i ciągłości działania w doskonaleniu organizacji* [at] Konferencja nt. Potencjał restrukturyzacji w warunkach globalizacji i nowej gospodarki. Akademia Ekonomiczna w Katowicach, Katedra Ekonomiki i Organizacji Przedsiębiorstw, 17-20.10.2007.

[23] Zawiła-Niedźwiecki J. - *Metoda TSM-BCP projektowania rozwiązań zapewniania ciągłości działania* organizacj [at] X Jubileuszowa Międzynarodowa Konferencja Naukowa nt. Zarządzanie przedsiębiorstwem. Teoria i praktyka, Akademia Górniczo-Hutnicza Wydział Zarządzania, Kraków 22-23.11.2007.

Information for Authors

Content of an article. A paper may describe original work, discuss a new method or application, or present a survey of recent work in a given field. Concepts and underlying principles should be emphasized, with enough background information to orient the reader who is not a specialist in the subject. A paper submitted to the Journal should not have been published elsewhere, including the World Wide Web, nor should it be submitted to another publication or to a conference concurrently.

Submission process. An article, prepared in MS Word, should be sent to Editor-in-Chief: prof. Tadeusz KRUPA, Faculty of Management, Warsaw University of Technology, ul. Narbutta 85, 02-524 Warszawa, Poland, e-mail: T.Krupa@wz.pw.edu.pl.

Review process. All manuscript are sent to two independent reviewers to ensure both accuracy and relevance to the journal. The final decision on acceptance will be made by the Editor-in-Chief.

Text. The manuscript must be produced clearly on plain A4-sized sheets - 210 by 297 mm. Set top and bottom margins for the pages at 25 mm. Set right and left margins as mirror margins with inside margin at 20 mm and outside margin at 16 mm. The body text must be printed in double columns with the middle margin of 8 mm. The body text is typed in 10,5pt Times New Roman with 1,15 multiple line spacing and 4pt spacing after paragraph. The title page should include the title of manuscript, author(s), affiliation(s), abstract (8 - 12 sentences) and key words (8 - 12 characteristic words).

References. References should be quoted in the text using consecutive numbers in square brackets, alternatively, as shown here [1, pp. 7-12], or [2, 4], or [1-3]. At the end of the manuscript, they should be cited as follows:

The monograph:
Author(s) - *Title of the monograph*. Publishing company, City and the year of the publication.

The example:
[1] Poe V., Klauer P., Brobst S. - *Building a Data Warehouse for Decisial Support.* Prentice-Hall Inc., New York 1998.

The monograph under the editing:
Author(s) (ed.) - *Title of the monograph*. Publishing company, City and the year of the publication.

The example:
[2] Ansoff H.I. (ed.) - *Corporate Strategy*. McGraw-Hill, New York 1965.

The chapter of the monograph under the editing:
Author(s) - *Title of the chapter* [in] Title of the monograph (ed. Authors). Publishing company, City and the year of the publication, numbers of pages.

The example:
[3] Wilson D.C. - *Organizational Structures in the Voluntary Sector* [in] Issues in Voluntary and Non Profit Management (ed. J. Batsleer, C. Cornforth, R. Paton). Addison-Wesley, Wokingham 1992, pp. 45-93.

The article in the journal:
Author(s) - *Title of the article* [in] Title of the journal, Volume, Number, year, numbers of pages.

The example:
[4] Barney J. - *Organizational culture: can it be a source of sustained competitive advantage?* [in] Academy of Management Journal, Vol. 28, No. 7, 1986, pp. 56-65.

The paper at the conference:
Author(s) - *Title of the paper* [at] Title of the conference, City and the year of the conference, numbers of pages.

The example:
[5] Bonits N. - *Intellectual Capital: An Exploratory Study that Develops Measures and Models* [at] The First Management Decision Conference, London 1998, pp. 12-20.

Editorial Office:
Teresa Ostrowska, email: T.Ostrowska@wz.pw.edu.pl
Katarzyna Rostek, email: K.Rostek@wz.pw.edu.pl

Faculty of Management
Warsaw University of Technology
ul. Narbutta 85, 02-524 Warszawa, Poland