# BUSINESS CONTINUITY MANAGEMENT IN THE BASE OF THE INTEGRATED SECURITY SYSTEMS

Prof. Dr. Eng. Kiril Stoichev, DSc. (Econ.)
HIGH-TECH IMS LTD
kstoichev@ims.bas.bg

***Abstract:*** *Different agencies and organizations engaged in the struggle against the terrorism use different approaches and tools for adequate response to the "plague of the century". Depending on the knowledge and skills of their employees they provide certain level of technical and operative readiness which guarantees them appropriate degree of security in relation to terrorist threats.*

*But is it this sufficient, are their efforts sufficient to guarantee that their reactions are adequate to the dynamically changing security environment?*

*This report attempts to answer this question through creation of a matrix of minimum and obligatory requirements for building a reliable counteraction system against potential terrorist threats, that should become the next step in the development of the theory and practice for application of Directive 2008/114/EO of the EC Council, is of significant importance for increase of the security and protection of critical infrastructure objects.*

**KEY WORDS:** BUSINESS ORGANIZATIONAL MANAGEMENT SYSTEM, BUSINESS CONTINUITY MANAGEMENT SYSTEM, INTEGRATED SECURITY SYSTEM, LEVELS OF SECURITY

## *1. Introduction*

During the past years at the international scene so many and different in content but identical by its nature events arise related to security which affect all parts of the world. They all to be described and classified is a difficult task. But main purpose of this material is not this. Our aim is not to examine the concrete processes in order to guarantee national or international security. Certainly, these efforts are important from the view point of formulating the frame of factors that affect security as a whole but our purpose is to focus on the problems connected with assurance of the critical infrastructure security and protection at objective level.

The degree of uncertainty and the necessity of protection significantly affect the economic and psychological expenses and lead to painful changes of the established norms of behavior and way of life.

In order that it becomes possible to achieve lasting and efficient results for overcoming the terrorist attack threat it is necessary the efforts to be purposive and focused on solving the problems in key places. And their solution can only be effective and efficient by using the systems approach and considering them as integrated connectivity in multiple subsystems.

As already noted when we talk about integrity of the critical infrastructure security and protection we have to specify the connecting link between the object individual components which in this case is the Business Continuity Management System.

The present section will examine this system through the prism of the Business Organization Management System. Each one critical infrastructure represents an original business organization and the style which is used for the presentation of the interconnections between the two systems should not seem strange to the reader. The following lines come to show not only the „heart" of the integrity in the management of one organization but also the way of thought that we should follow in the creation of the integrity of the security and protection of the respective objects.

In the present report such attempt will be made to determine the role of the Business Continuity Management System in the Management System for business organization activities, i.e., we shall try to show the interconnections of the former with the system components of the latter without having the ambitious notion to determine its place between them. And this is not the purpose. With the indication of these interconnections we aim at laying the beginnings of the manner of thought and action for creation of integrity of the critical infrastructure objects security and protection as function of the activity of the Business Organization Management System.

## *2. Components of the Business Organization Management System*

The starting point for the organization when it specifies the parameters of building its management system frequently has been the necessity for ensuring compliance with the external for the organization standard. Thus for instance, the organizations rather set for their purpose to develop "Quality control system" or "Environmental control system" on the base of the respective standard structure than logically to determine how they work and what are the interconnections between them.

Similar manner of thought and action results in the presence of many systems in one organization built according to different standards and independently taken alone. This is economically inexpedient and frustrating and just on that basis the international standardization organization has come to the conclusion that these standards should have general format, general structure. ISO 9001:2000 is used as model for many other standards but unfortunately still there is a tendency for using only the shaping of the standard itself as point of reference for description and structuring the management system.

The conventional approach which is currently adopted by many theoreticians and practitioners is determination of rights and responsibilities with respect to the aspects of the individual systems that form the business management system, to be done separately for each one of the systems. The tendency is already to pass over to integrated management systems particularly when the respective company wishes to be certified for compliance with the requirements of more than one standard.

The term „integrated management" has to be synonym of „good management" which means that it is necessary to manage the organization activities, resources, personnel, the influences on its function as well as the numerous risks that may cause many more problems if permitted to be realized than if they are avoided.

Such an "aggregate" image of "integrated management" is Integrated Management System.

## *3. Business Continuity Management*

The Business Continuity Management (BCM) entered in the field of the critical infrastructure security and protection after 2009 **[1]**.

The area of the business processes continuity contains in itself managerial activities and integrated plans that create conditions for maintenance of continuity of the critical for certain organization processes **[2]**. This area envelopes all aspects of one organizational unit which participate in the maintenance of the critical processes, that is to say: the personnel; buildings; suppliers; technologies; data. Its determinative role particularly strengthens when the

guaranteeing of the critical infrastructure objects continuous function is concerned.

Just on the base of the above presented we shall attempt to define the interconnections of the Business continuity management system (BCM system) with the remaining subsystems of the Business organization management system.

## *4. Interconnections between the BCM system and the subsystems of the Business Organization Management System*

In order to determine these interconnections we shall try to point out the similarities and differences with respect to the requirements to creation of Business Organization Management System and the Management Systems of: the quality, environment, health and labor safety, finances, human resources, information technologies and data protection, corporate social responsibility, risk control (although the last system should not be considered an independent one but as a process which supports the creation and progress of the remaining systems) **[3].**

**But which are the similarities?** The building of the above said systems requires creation of specific for the individual field of activity of the business organization documents or performing actions such as: policy; strategy for realization of the formulated in the policy main courses for development; risk analysis; detailed plan for the realization of the strategic purposes and tasks; actualization, maintenance and test of the plan; training of the personnel for fulfilment of the individual modules and tasks of the plan; carrying out preventive and corrective actions, regular monitoring of the business environment changes and audit of the activities related to achievement of the set in the policy and strategy purposes. The methodology used is either identical (quality, environment, health and labor safety) or similar and very close (finances, human resources) which provides conditions for understanding of the organization general and specific problems by most of its workers and employees. But in spite of this, that fact is still not sufficient for the complete realization of the integrity of the Business Organization Management System and its System components.

**Which are the differences?** The substantial difference between them is carrying out the Analysis of the impact on the business in the course of building the Business Continuity Management System.

The purpose to prepare Business Impact Analysis for every action, process, product or service is to:

- document the effects that could arise as a result of loss or interruption of the organization/system activity;
- specify the time necessary to restore the respective function;
- specify the conditions (external or internal) necessary for the system/organization to function efficiently.

The above said is at the basis of the difference between the Business Impact Analysis and the Risk Analysis, i.e., the former examines the events which lead to significant interruptions of the activity while the latter considers all potential events that could affect the organization business. Both analyses are determinative for the creation of the policy and strategy of business continuity management. Precisely the last one is also another aspect of the differences that exist for the requirements of the BCM system and the identified above subsystems – presence of complex and detailed assessment both of the critical for the activity of certain organization factors and of the complete set of threats, general and specific, for the individual business lines.

As noted at the beginning the connecting sector between all these areas have become the standards of the ISO 9000 series. And indeed the quality in the management activities of: the environment, health and labor safety, human resources, information technologies and data protection, corporative social responsibility, risk, is immanent nature of them and by the structure and methodology of these standards a good attempt was made for synchronization of the efforts in the business organizations. But nevertheless the management of the finances is hinted in the standardization requirements, with respect to the quality in the organization activity, the management of this business sphere has its own entirely different requirements and methodologies.

On the other hand, the information technologies management and data protection has „impregnated" the entire business organizations activity no matter in which sector of the economy they function. And that is because not only that the 21Century is the century of the information technologies but also because they are in the base of, and before all, the finances management. But they are not so committed and not a critical factor for the management of part of the other subsystems, for instance the corporate social responsibility.

In order to elucidate what is this responsibility we shall point out the following example from the recent USA history (which presents a clear notion of the importance of the communication-information technologies and corporate social responsibility). The finance and credit institution Cantor Fitzgerald occupies floors from 101 to 105 in one of the World Trade Center towers. These are two floors above the zone where the first airplane hits the Towers on 11 September 2011 **[4].**

Immediately after the first attack on 11 September, approximately at 8:46:46 in the morning, six seconds after the first airplane hits the tower, the Goldman Sachs server of electronic trade sends a signal page with information that the Goldman Sachs server has established connection with a backup server because there is no possibility to establish connection with the Cantor Fitzgerald server.

Cantor Fitzgerald lost all the employees in this building during the attack, 658 employees (approximately two thirds of the company personnel), which includes brokers, tradesmen, experts and secretariat.

The executive manager and chairman of the board Howard Lutnick whose brother is among the perished gives an official promise to keep the company "alive". The lately developed by the company system of electronic trade is immediately set in motion in order to replace the perished brokers and tradesmen. This way the company is in position to regain its online markets within the frames of a week (even their competitors help them in this undertaking).

On 19 September 2001 Cantor Fitzgerald assumes the engagement to grant 25 % of the company profit in the following five years for compensations as well as in the frames of the next ten years to pay the health insurance of the families of the perished 658 their former employees. In 2006 the company fulfils the promise paying more than 180 million dollars to the families of their former employees.

Before the attacks Cantor occupied approximately one fourth of the everyday transactions in the multi milliard market of securities. The company restored its infrastructure and currently has offices in midtown Manhattan and there work more employees than before the attack.

And all these in a considerable degree is due to the precisely developed, flexible and successfully and professionally applied Business continuity management system of the company. In the developed for the purpose policy, strategy and plans both vision and requirements to the communication-information system for ensuring their continuous operation in emergency or crisis and concrete purposes and priorities concerning the corporate social responsibility of a business organization have found place.

But not only this example shows the connecting sector between two of the subsystems of the integrated management system and this sector appears to be the BCM system.

In practice there is no other subsystem besides the BCM system which in one way or another comprises compulsory requirements with respect to the remaining subsystems of the business organization management system.

Thus for instance, the BCM system possesses absolutely all components of the structure of the quality management system

(which is fundamental in accordance with the ISO standards for management systems) and uses its methodology in the process of its own building. Placing requirements for the management subsystems of the environment, health and labor safety, human resources, information technologies and data protection, corporative social responsibility, risk control is an obligatory condition in the development of the BCM policy, strategy and plans. And most of all, the requirements to the management of the financial subsystem of the Business organization management system occupy a serious sector of this system (in contrast to the quality control where the requirements are only cursorily referred to). The requirements to this subsystem refracted through the requirements to the communication-information systems are so detailed and purposive that sometimes the experts could ask themselves the question „Has the BCM system been created by any chance solely and only to support and guarantee the continuous function of the Finance management system?"

## *5. Critical Infrastructure Security and Protection Levels*

This section is the essence of the methodology for building integrated critical infrastructure security and protection. It logically follows the preceding section which examines the problem of the central role of the BCM system as an integrating, connecting unit in the Organization Management System and presenting the "heart" of the integrity of the respective object security and protection.

The Conception of the critical infrastructure security levels presented here **[5]** considers that the Management System of certain organization consists of multitude of subsystems that separately realize the different organizational functions. If these subsystems are projected on the organization security and protection sphere we can with sufficient degree of certainty say that the picture presented in Figure 1 would be obtained.

The Figure is an attempt of visualization of the interdependences between the organization management system individual components. Certainly, these components are not fixed and their number may be increased or decreased, respectively, this being dependent on the analytical cross section that we have made a purpose of examination (thus for instance, the financial security, from the view point of security it could belong to the information security considering its direct dependence on the information systems).

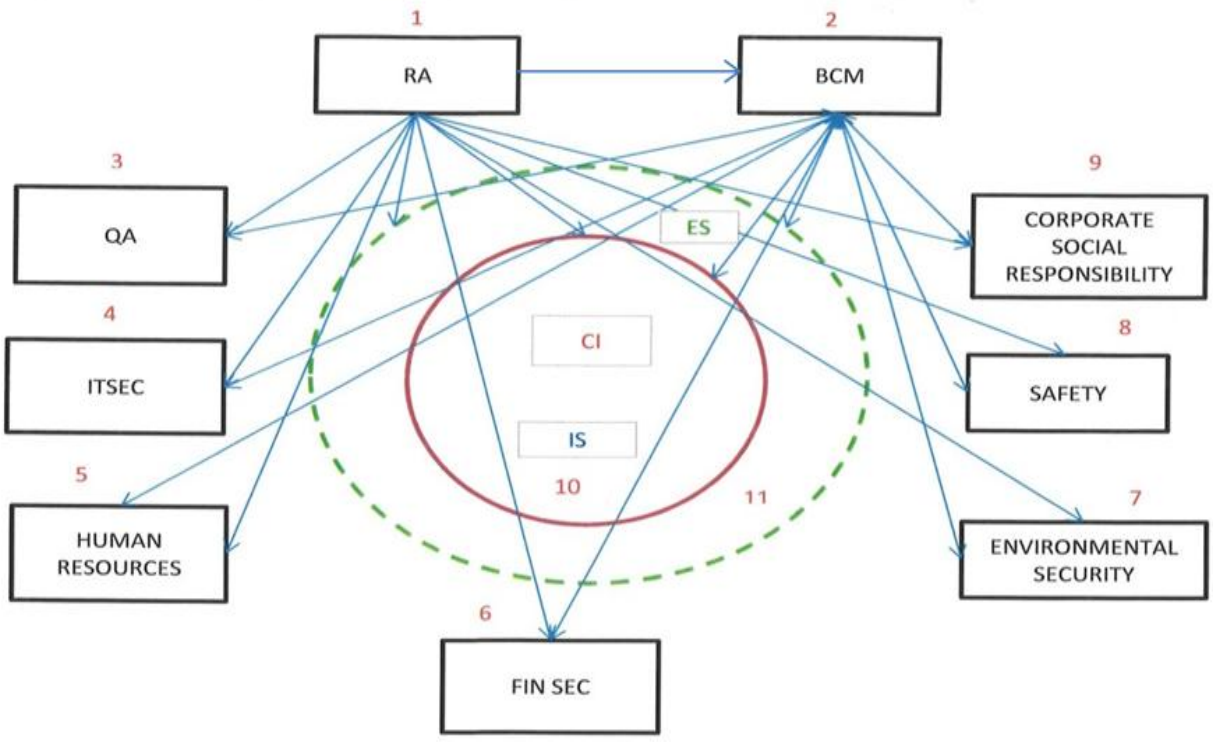


***Figure 1*** *Management system through the security prism*

**Legend: RA** – Risk Assessment; **BCM** – Business Continuity Management; **QA** – Quality Assurance; **ITSEC** – Information Security; **FIN SEC** – Financial Security; **CI** – Critical Infrastructure; **IS** – Internal Security; **ES** – External Security.

First of all, probably everybody will agree, input signal for building modern subsystems of the management system are the results of carrying out the Risk Assessment. And the connection is unidirectional – from RA to every one of the subsystems. And that is because RA is the source of information concerning what is the probability of certain event to happen which provides the possibility for the corresponding subsystem to undertake the necessary preventive or corrective measures to ensure the stability of its function. As far as the fact that the connection is unidirectional it is obvious that the source of information for RA is the organization environment which presents data about potential threat for one, several or all together management subsystems (here we accept the limitation that we speak about the beginning of building these subsystems because if they are already built, the situation is different, RA receives information also from the process of their functioning, not only from the environment).

In the same time the interrelations between the Business Continuity Management and the remaining subsystems are bilateral (in the general case BCM is built after the remaining systems have been built). The input signal for the rest of the subsystems is the Business Impact Analysis (BIA), and the reciprocal connections of every subsystem to BCM are concretized by the data about the condition

of the subsystems critical components (it is well known that RA is engaged with all potential threats while BIA assesses only the critical for the system components).

The Figure presents only the connections between RA and BCM without attempt to illustrate the connections between the remaining subsystems. The grounds for this is the risk of shifting the focus from the set purpose –systematization of the individual subsystems in levels of complete/integrated security and protection of the critical infrastructure object.

## *Conclusions*

The presented above detailization of the security components/levels where in the center of which is placed Business Continuity Management System aims first of all, but not only, at creation of conditions for enhancement of the critical infrastructure objects security and protection. Certainly, the last said may be achieved in different ways the main of which, according to some experts, is improvement of the equipment and technologies that are used in this sphere. But this is an isolated situation from the suggested here integration approach. The technologies in themselves are not in condition to do anything if they are not controlled. And this is the greatest confirmation of the statement that security is ensured by the joint use of technologies and organizational procedures for their control, the two taken together and unified by individual components or complete security and protection systems.

The determination of individual security levels in these systems is fundamental criterion for assessment of the degree of trust to the organization, which the systems can and have to generate in the users of their services and in the society as a whole. Confidence which could be materialized, besides by all the other, and by the insurance system that is its objective measurement. But before going so far it is necessary to develop detailed requirements to each one of the above said security levels which later on to be in the base of created for the purpose international standardization documents. The development of the equipment and technologies separately for the corresponding subsystems is not enough to provide our security. Therefore, the clever combination between them coupled with the best practices from the management can create a flexible, reliable medium for using various combinations of means and as a result a synergetic effect of their use to guarantee the required security level of our organization.

We do not pretend that the thus suggested structure and content of the security levels are precisely those that will remain in the future and are precisely those that could form this confidence both in the organization managements and in the society. But we are firmly convinced that such levels must exist! The mechanism of their application could follow the already known approach adopted by the International Standardization Organization – development of standard/s with requirements for these levels and standard/s for audit and certification of them. Only this way we shall be able to say that we have passed to the next stage of development in direction of guaranteeing more and more high reliability of our efforts to preserve the way of life we have chosen – the democracy.

## *References:*

**[1]** Stoychev K., System for effective business continuity management, Published by UNSS, March 2013, ISBN 978-954-644-470-7.(In Bulgarian)

**[2]** Stoichev K. (2012), Conditions for Increasing of the Viability of Critical Infrastructure Objects, Journal of Applied Security Research, Volume 7:4, 409-416, (ID: 710131 DOI:10.1080/19361610.2012.710131).

**[3]** Stoichev K., (2014), The Role of Business Continuity Management in the Business Management System, Science Journal of Business and Management, 2(3), 97-102, DOI: 10.11648/j.sjbm.20140203.12, ISSN: 2331-0626 (Print); ISSN: 2331-0634 (Online).

**[4]** ECP – 601: Effective Business Continuity Management, Institute for Business Continuity Training, US.

**[5]** Stoichev K., (2014) Security Levels of Critical Infrastructure, Journal of Applied Security Research, Volume 9:3, 328-337, DOI: 10.1080/19361610.2014.913233.