# STANDARTIZED APPROACHES FOR INTEGRATION OF MANAGEMENT SYSTEMS FOR OBJECTS OF THE CRITICAL INFRASTRUCTURE

**Dimitar L. Dimitrov, Valeri S. Panevski**

*Institute of Metal Science, Equipment and Technologies "Akad. Angel Balevski" with hydro and aerodynamics center - Bulgarian Academy of Sciences*
*1574 Sofia,"Shipchenski prohod" blvd. № 67*

STANDARDIZED APPROACHES FOR INTEGRATION OF MANAGEMENT SYSTEMS OF CRITICAL INFRASTRUCTURE SITES

**Dimitar L. Dimitrov, Valeri S. Panevski**

*ABSTRACT: Over the past few years by the International Organization for Standardization (ISO), were developed different standards for management systems, aiming to manage different sectors of activities of organizations (businesses). Practice shows that despite many common components, they are not sufficiently coordinated, which hinders stakeholders to streamline and integrate their management systems. That`s way, in this paper, authors will present a systematic research process of integration texts into existing standards, in the area of requirements for Management Systems and especially for the Business Continuity Management, with the leading role of Quality Management System, in the organizations which essentially represent objects of critical infrastructure.*

*KEY WORDS: quality management system, business continuity management; critical infrastructure, security and protection.*

## 1. Introduction

In 2011 International Organization for Standardization (ISO) developed and promulgates its ISO Guide 83 – "High level structure, identical core text and common terms and core definitions for use in Management Systems Standards." - ISO JTCG N 316 - December 2011, which provided guidelines for the development of Management Systems **[1]**. As a consequence of this fact, the also publicated in our country standard БДС EN ISO 22301:2015 - "Security of society. Systems for Business Continuity Management. Requirements." is pilot in this area and prepared in accordance with the requirements of Guide 83 **[2]**.

Traditionally, and following the best practices, nowadays are developed individual enterprise management systems, to address issues such as quality, environment, health and safety, finance, human resources, information technology and data protection. Other key aspects of the activities of the organization/object of the critical infrastructure (CI), which also require the establishment of management systems include corporate social responsibility, security of data, management of risks and continuity of business/activities (Business continuity).

What dictates the necessity to create a Business Continuity Management System for objects of the CI?

Business Continuity - processes and systems incorporate management activities and integrated plans that create conditions for maintaining the continuity of critical for an

organization/object of the CI processes **[3].** This area covers all aspects of an organizational unit involved in the maintenance of critical processes, namely personnel; buildings; suppliers; materials; technology; data. Its decisive role is especially serious when it comes to ensuring the continuous operation of critical infrastructure, especially those identified as such in the energy and transport sectors.

## 2. Nature of the problem

There are numerous approaches, ways and means to create conditions for continuous operation of such infrastructure, which in varying degrees affect their specifics. From there are different degrees and levels of security to ensure the continuity of their business development.

Rounding out the theory and practice of planning continuous business development and exchange of experiences and good practices, contribute to increase the security of the economic or organizational entities, but the lack of a model for identical objects gives rise to uncertainty in terms of degrees of their viability, ie, no objective criteria to compare and assess the degree of resilience of the site in different critical situations.

Considering the fact that such objects are the basis of the critical infrastructure of all member states of the European Union it is essential to create conditions for a reliable assessment and achieving the required extent and level of security to ensure the continuity of their development.

Natural disasters, environmental emergencies, technological mistakes and crises caused by human factors, indicate that severe accidents can and will happen, which affects both the public and private sector. The challenges go beyond the scope of the plans for emergency responses or the disaster management strategies.

Organizations of all types and sizes, especially those who enter the category of critical, need to engage in a comprehensive and systematic process of prevention, protection, preparedness, mitigation and response to ensure business continuity and its recovery. It is no longer enough to prepare a response plan that provides for the minimizing of the effects of natural, accidental or deliberately caused suspensions of the activity. Rather organizations including and objects of the CI should take adaptive and innovative measures to reduce the likelihood of the realization of such an event. Modern threats require the creation of a continuous and controlled process that ensures the survival and sustainability of the main activities of the organization/object of the CI before, during and after a devastating event.

Organization's ability to recover from the effects is directly related to the degree of business continuity planning prepared before the event. Studies show [1], that two of five companies, that came under the impact of a disaster, will go out of business for a period of five years. Plans for business continuity are critical to all businesses. More importantly, these plans become increasingly important as companies become more trusting towards technology for doing business.

Despite the clear message that downtime is catastrophic, the researches of "Gartner" (an American company carrying out researches in the field of information technology and consulting services) show that less than 30% of companies in the "Fortune 2000" (ranking of global companies in: performance marketing, profits, assets and market value) have invested in comprehensive plan for business continuity. One of the possible

[1] *Whitepaper ISO 22301 Societal security. Business continuity management systems.*

reasons for this omission is that the technical challenges seem too confusing or maybe that the costs for developing the plan seem too large. БДС EN ISO 22301 is the world's first international standard of requirements for Business Continuity Management Systems (BCMS), which was developed to help organizations minimize the risk of such violations.

### 3. Factors determining the need to create and use standardized Business Continuity Management Systems (BCMS).

As is known, serious accidents can and will happen, a circumstance which affects both the public and private sectors of every society, at the same time challenges beyond the scope of plans for emergency response or disaster management strategies.

In order to increase the level of security and protection of CIs, it is not enough to prepare a response plan that provides for minimizing the effects of natural, accidental or deliberately caused interruptions of business, but rather need to take adaptive measures to reduce the likelihood of the realization of such an event. In practice, there is no other subsystem besides Business Continuity Management System, which in one way or another includes mandatory requirements in relation to the other subsystems of the single Management System of the organization.

In the presentedup to here may with reasonable certainty be stated that there is a new global policy aimed at developing standards for Management Systems, through unified and consistent high level of structure, identical text, general terms and basic definitions, mainly based on the principles, requirements and standardized approaches of БДС EN ISO 9001:2008 - "Systems for quality management. Requirements.", a requirement which are the basis of all systems related to the activities of the organization/object of the CI **[4]**.

For example, the System for managing business continuity has absolutely all the elements of the structure of the management system for quality (which is fundamental, according to the standards of the International Organization for Standardization for Management Systems (MSS) and uses its methodology in the process of building its own. As pointed out above, claims to the requirements for subsystems for environmental management, health and safety, human resources, finance, information technology and data protection, corporate and social responsibility, risk management, are prerequisite for the development of policy , strategy and plans for this system.

There are several standards for managing business continuity worldwide, while this matter is seen as a relatively new. One of the leading documents is the standard БДС EN ISO 22301:2015, which applies to all organizations, including and sites of the CI, irrespective of their type and size, and wishing to:

- establish, implement, maintain and improve BCMS;
- confirm compliance and continuity with the declared policy of the organization to ensure business continuity;
- demonstrate to other organizations compliance of their activities with the requirements of this standard;
- seeking certification/registration of its BCMS by an accredited third party;
- seek self-determination and declaration of compliance with this international standard.

As with all significant actions within the organization, it is necessary to obtain the support of the senior management. By far the best way to achieve this goal is instead to

point out the negative aspects of the lack of process for business continuity management (BCM) to promote the positive achievements of owning a build in process for effective BCM. Today the good business continuity management does not mean, to take forced measures against external influence, but rather recognition of the positive effects of the use of best practices for business continuity, shown in Fig. 1, which are created in the organization **[5]**.

| | | | |
|---|---|---|---|
| Predictable and effective response to crisis | Protection of personel | Maintain of vital for the organization activities | Better understanding of the organization |
| Reduce of costs | Respect to the stakeholders | Protection of the reputation and the brand | Client trust |
| Competitive advantage | Legislation compliance | Regulatory compliance | Contract compliance |

**Fig. 1 Best practices in the field of Business continuity.**

The adoption of effective BCM process is beneficial in a number of areas of activity of the organization, including:

- protection of assets (property);
- improve understanding of the business, achieved by identification and analysis of risk;
- оперативна устойчивост, постигната като резултат от прилагането на подход за намаляване на риска;
- reduce of the interruptions by defining alternative processes and ad hoc approaches to respond to unforeseen problems or risks;
- related approaches that can identify and manage alternative processes;
- vital records and data that must be maintained and protected;
- effects of legislation on health and safety, and obligations for care of the staff;
- improved operational efficiency through compulsory program for re-engineering of business processes;
- protection of the physical assets of the organization;
- keeping the markets, ensuring continuity of supply of goods and services;
- improving the overall security of the organization (the site of the CI).

Taking the decision to develop BCMS based on БДС EN ISO 22301:2015, is usually acceptable, as the benefits are well documented. Most organizations now realize that it is not appropriate to apply a unified plan to ensure business continuity of all elements. To create conditions for giving an effective response in terms of maintaining operational continuity, such a plan must be customized to the specific risks and catastrophic scenarios that could range from loss of a major building to a local fault in the system for the implementation or maintenance of the core activity. A more difficult task is the development of an implementation plan to balance the requirements of the standard, the business needs and the deadline for certification.

There is no single plan for the implementation of БДС EN ISO 22301:2015, that will work for any organization, but there are some general steps shown in Fig. 2 and Table 1 that will allow balancing the often conflicting requirements.

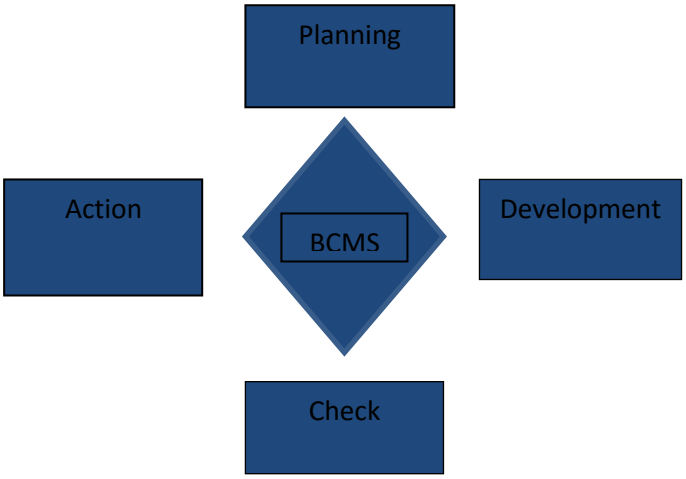


**Fig. 2 General steps to implement БДС ЕН ISO 22301**

The following Table 1 shows the general steps and activities associated with them for the implementation of БДС EN ISO 22301.

**Table 1 General steps and related activities for the implementation of БДС EN ISO 22301.**

| *1. Planning* | *2.Development* | *3.Check* | *4. Action* |
|---|---|---|---|
| **1.1. Start of the development of BCMS** | **2.1.** Strategy for BC | **3.1.** Monitoring, measurement, analysis and evaluation | **4.1.** Removing inconsistencies |
| **1.2. Understanding of the organization** | **2.2.** Organizational structure | **3.2.** Internal audit | **4.2.** Continuous improvement |
| **1.3. Analysis of the existing system** | **2.3.** Document Management | **3.3.** Management review | |
| **1.4. Leadership and project approval** | **2.4.** Protection and measures to reduce the impact | | |
| **1.5. Goal** | **2.5.** Plan for BC and procedures | | |
| **1.6. Policy for BC** | **2.6.** Communication | | |
| **1.7. Analysis of the impact on continuity** | **2.7.** Training and awareness | | |

| | |
|---|---|
| **1.8. Risk Assessment** | **2.8.** Training and checking |

БДС EN ISO 22301:2015 is a document of a new type, which is realized at the highest level of complete integration of structure and text, in full compliance with the ISO Guide 83 for Standards for Management Systems. It was prepared in response to the critics, that so far as current standards have many common components they are not sufficiently coordinated, making it difficult for organizations to streamline and integrate their management systems.

## 4. Management of quality and business continuity - system integration compliance between БДС IN ISO 9001:2008 and БДС EN ISO 22301:2015

БДС EN ISO 9001:2008 does not include requirements specific to other management systems - environmental management, management of health and safety at work, financial management or risk management. However, this International Standard enables an organization/object of the CI to coordinate or integrate their own System for Quality Management with requirements of the applicable system for Business Continuity Management. It is possible that the object of the CI adapts its (their) existing Management system(s) to develop a System for Quality management, corresponding to this International Standard.

On the other hand, as was underlined, it is important to know that through БДС EN ISO 22301:2015 is introduced an application cycle "Planning - Development - Check - Action" (PDCA) in the construction of BCMS. Thus ensuring a degree of consistency with other standards for Management systems, such as: БДС EN ISO 9001:2008, БДС EN ISO 14001:2005 – " Management systems in relation to the environment. Requirements and guidelines for implementation.", БДС ISO/IEC 27001:2014 – " Information Technology. Security methods. Management Systems for information security. Requirements. ", БДС ISO/IEC 20000-1:2012 – " Information Technology. Service Management. Part 1: Requirements for management system for services." and БДС ISO 28000:2012 – " Requirements for Systems for Security management of the supply chain.". This allows to create conditions to ensure the consistency and integrity in the construction and implementation of the separate management systems.

Table 2 shows the integration compliance between standards ISO 9001:2008 and ISO 22301:2015.

**Table 2 Integrational compliances**

| Requirements | БДС EN ISO 9001:2008 | БДС EN ISO 22301:2015 |
|---|---|---|
| **Objectives of the Management system** | *5.4.1* | *6.2* |
| **Policy of the Management system** | *5.3* | *5.3* |
| **Commitment of the leadership** | *5.1* | *5.2* |
| **Requirements for documents** | *4.2* | *7.5* |
| **Internal audit** | *8.2.2* | *9.2* |
| **Continuous improvement** | *8.5.1* | *10* |

| | | |
|---|---|---|
| **Improvement - management review** | *5.6* | *9.3* |

## 6. Conclusion

From the above it is clear that a fundamental standard for management systems appears to be БДС EN ISO 9001:2008. This means that the timely installation and full size functioning of the System for quality management, in an organization, creates an appropriate basis for the implementation of Business Continuity Management System.

Namely providing business continuity of any organization/object of the CI is theory and practice, which originated in not very long. Therefore, the try to show ways and means to integrate the system, that is built in to solve the issues related to business continuity, is definitely a logical and up. This on the one hand will allow to determine its place in the palette of systems, forming the content of a single Business continuity management system for each company or entity of the critical infrastructure and on the other hand, will determine the contribution that this system can provide for meaningful, sustainable and continuous meeting of the needs of those who consume their services/products.

## References:

**[1]** ISO Guide 83 High level structure, identical core text and common terms and core definitions for use in Management Systems Standards. - ISO JTCG N 316 - December 2011.

**[2]** ISO 22301, Societal security. Business continuity management systems. Requirements.

**[3]** Stoichev K., Conditions for Increasing of the Viability of Critical Infrastructure Objects, Journal of Applied Security Research (ID: 710131 DOI:10.1080/19361610.2012.710131).

**[4]** ISO 9001, Quality management systems. Requirements.

**[5]** Stoichev K., Dimitrov D., Panevski V., ACTUAL APPROACHES FOR MANAGEMENT SYSTEMS INTEGRATION ELABORATED ON THE BASE OF ISO STANDARDS - ISO 22301:2012 and ISO 9001:2008, Seminar ”Development of a methods and criteria for examination, analysis and assessment of the adjoining to the airport areas. Development of a security and protection model of the airport external perimeter”, HOME/2010/CIPS/AG/019, Sofia Airport, 15 March, 2013.