RISK ASSESSMENT MODEL BASED ON ISO 22301:2012 "SOCIETAL SECURITY. BUSINESS CONTINUITY MANAGEMENT SYSTEMS. REQUIREMENTS"

Ilia Tzenev[1], Georgi Popov[3], Mariana Shirkova[2]

[1]Practice Q.A. Ltd. 23, Bulgaria

[2]"QUALITY 21-st CENTURY" Foundation, Bulgaria

[3]University of Central Missouri, USA

Abstract

The report examines the main aspects of ISO 22301 standard. Comparative analysis of ISO 22301 and the main management systems standard ISO 9001 is discussed. Emphasis is placed on the fact that the implementation of systems under ISO 22301 is a meaningful assessment of the risk to the society while maintaining "business continuity" in societal structures.

Key words: *management systems, risk assessment, business continuity*

1. INTRODUCTION

The first version of ISO 9001 was published in 1987. In 1994 the second version followed, which also applied more structured approach to implementing and maintaining quality systems. In 2000, a new version, in which for the first time applied the process approach in the implementation and maintenance of management system (MS) quality. The next version, published in 2008, continued with the MS process approach. Based on ISO 9001, ISO published Environmental Management System standard ISO 14001. The second version of this standard came out in 2004. It should be noted that after 2004 the active adaptation of ISO 9001, was not only applied to the environment, but also for food (ISO 22000:2005), information security (ISO/IEC 27001:2005), and energy efficiency (ISO 50001:2011). One of the recent developments of ISO 9001 logic is an ISO 22301:2012 "Safety of society. Management systems business continuity. Requirements". This standard is suitable for management, business processes and political processes (the first ISO-standard offering good practice for political parties and other organizations dealing with policy).

SM quality model by applying the process approach

Fig. 1 shows the universal model, pioneered by ISO 9001:2000. Shown in the diagram is an ISO 9001:2008. As stated above the MS model described in ISO 9001:2000 is identical to that of ISO 9001:2008. ISO is currently updating the latest version of the standard and it is expected to come out in 2016. In it, pattern shown in Fig. 1, is also preserved, which can be seen from the published draft ISO DIS 9001:2014.

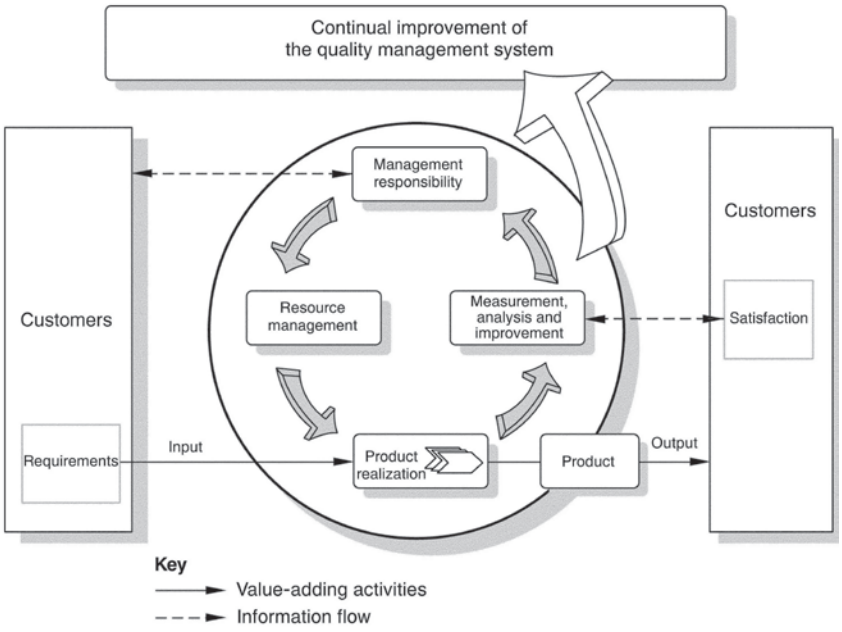


Fig.1

Fig. 1 model has the following characteristics:

- All MS activities are regarded as processes that are interrelated. The output from one process is one or more inputs of the other processing;
- For each MS the 8 principles introduced in ISO 9000:2000 are valid. Principles are preserved in the latest version ISO 9000:2005;
- Maintaining and improving the SM applicability of the ISO 10000 standards. The most popular (ISO 10002, ISO 10003, ISO 10004, ISO 10005, ISO 10008, ISO 10012, ISO 10013, ISO 10014, ISO 10017) are issued translated into Bulgarian, by the Bulgarian Institute for Standardization.

The authors experience shows that the interested parties in Bulgaria do not benefit from those standards in the ISO 10000 series. The standards are available at: www.iso.org. Not implementing good work practices recommended by MS in the ISO 10000 leads to failure of management principles of ISO 9000:2005. This leads to a degradation or a complete lack of efficacy and effectiveness of the model of fig. 1 in its realization in concrete MS according to ISO 9001:2008 or if the system is working with other systems (ISO 14001, ISO 27001, etc.) in the "Integrated Management System".

In connection with the above finding, and other shortcomings in the implementation/certification of the MS, the authors have a number of critical publications. They show "boom" of MS certifications after 2000. The main reason is the set requirements for public procurement candidates to furnish proof of their certified management systems for quality, environment, food safety and others. The results obtained from this "bad Bulgarian practice" are prominent - our country ranks last in positive indicators for social development, and is ranked first in terms of negative indicators. The authors hope the terms "positive" and "negative" indicators are quite understandable, without the need to specify specific names.

Short introduction of ISO 22301:2012

Fundamental concept of this standard is "business continuity". It should be viewed as the ability of the organization (profit or non-profit) to continue to supply products and / or services of acceptable preset levels after a devastating accident. This standard can be applied by political parties. Unlike the published ISO-standards for MS, this standard together with ISO 27001 is an efficient and effective tool for maintaining continuity of political parties after the election defeat or inappropriate performance management (destructive political incident). International and Bulgarian and practice

have shown that in such incidents, the affected political party cannot restore its work for a long time. Similar recommendation for using ISO 22301:2012 can be made to rating agencies or other organizations involved in the political process. The above statement also applies and after a devastating political incident, their activities are significantly reduced or the incident can lead to interruption of operations.

In connection with the above stated principles, in the interest of public safety, the development of which is determined by the business and political processes, by this standard helps application/certification "Business continuity management system" (BCMS). Implementation of BCMS stresses the importance of:

1. Understanding the needs of the organization and of the need to establish policy and objectives for the management of business continuity;
2. The introduction and implementation of mechanisms for control and management measures the overall ability of the organization to manage in destructive incidents;
3. Monitoring and review of the performance and efficiency of BCMS, and
4. Continuous improvement based on objective measurement.

As with any management system ISO-standards and BCMS have the following main elements:

- Policy
- Staff with certain responsibilities
- Management Processes related to:
    - policy
    - planning
    - implementation and operation
    - evaluation of performance
    - management review
    - improvement
- Documentation providing suitable audit evidence
- All processes for managing business continuity applicable to the organization

Business continuity contributes to more flexible society. The wider community and the environment, in which the organization operates, affect the organization and therefore may need other organizations to participate in the recovery process.

Business Continuity Management System Model

Fig. 2 shows the pattern of a Management System. The scheme is included in ISO 22301:2013. It is obvious that to a great extent the system is close to the model in Figure 1. In the standard, this model is called " planning - implement - check - act ". This stems from the English "plan-do-check-act" (PDCA), introduced as a principle in Total Quality Management from the American scientist W. Edwards Deming (10.14.1900 -20.12.1993). In the ISO 9000:2005, this principle corresponds to the principle of "continuous improvement" of the Management System, which in practice is carried out by applying the PDCA.

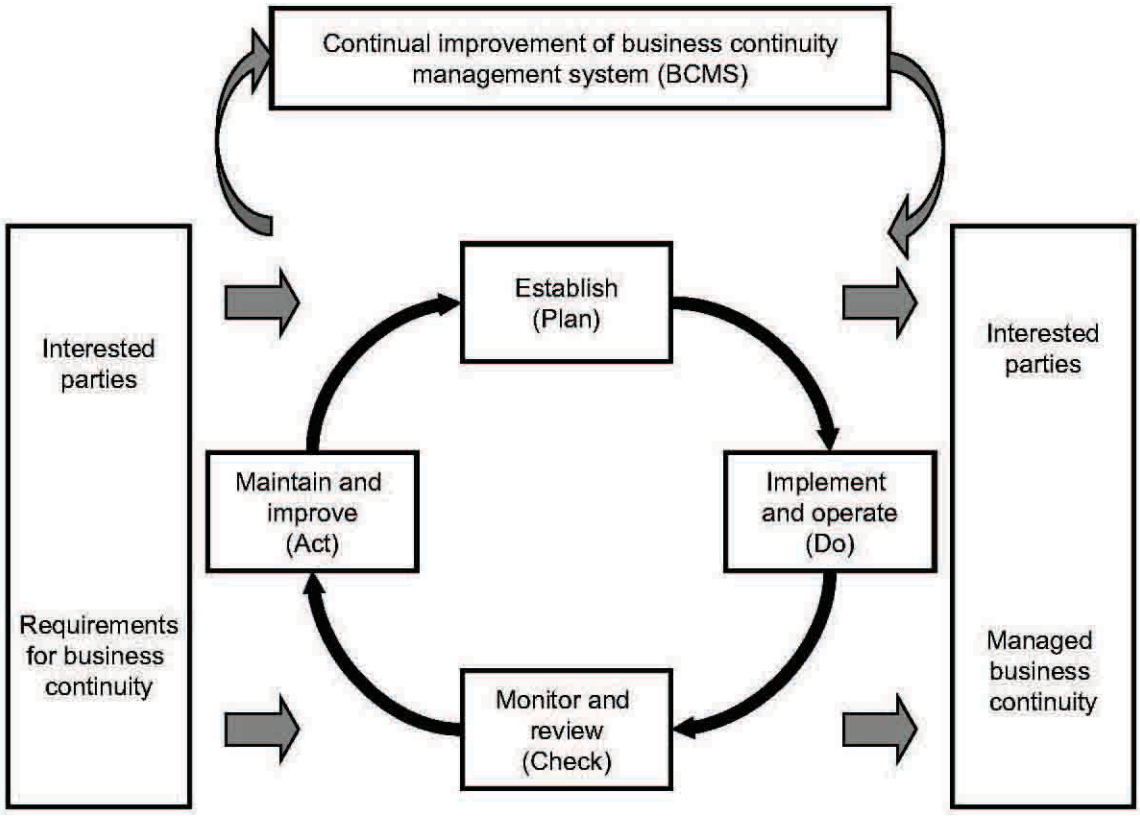


Fig. 2

Plan (Establish)	Establish business continuity policy, objectives, targets, controls, processes and procedures relevant to improving business continuity in order to deliver results that align with the organization's overall policies and objectives.
Do (Implement and operate)	Implement and operate the business continuity policy, controls, processes and procedures.
Check (Monitor and review)	Monitor and review performance against business continuity policy and objectives, report the results to management for review, and determine and authorize actions for remediation and improvement.
Act (Maintain and improve)	Maintain and improve the BCMS by taking corrective action, based on the results of management review and reappraising the scope of the BCMS and business continuity policy and objectives.

Fig. 3

The model, "Planning - Implementation - check - act" , as shown in the table in Fig. 3 and in Sections 4 to 10 of ISO 22301:2012, includes the following elements:

- Section 4 is an element of planning. Section 4 introduces requirements that are necessary to establish the context of the BCMS, as regards the organization and the needs, requirements, and coverage.
- Section 5 is an element of planning. The section summarizes the specific requirements of the role of senior management in the BCMS and the way in which management expressed their expectations through policy statement of the organization.
- Section 6 is an element of planning. The section describes requirements, which relate to the definition of strategic objectives and guiding principles for BCMS general. The content of Section 6 differs from creating opportunities to influence the risk arising from the risk assessment and an analysis of the impact on activities derived from the purpose of recovery. The analysis of the

impact on business and process requirements for risk assessment are described in detail in Section 8.

- Section 7 is an element of planning. It supports actions of BCMS, as they relate to the definition of competences and the exchange of information on repeated necessary with stakeholders during the documentation, management, maintenance and preservation of the necessary documentation
- Section 8 is an element of performance. It specifies requirements for business continuity determines their direction, to develop management procedures in a devastating accident.
- Section 9 is a verification element. It summarizes the requirements that are needed to measure the effectiveness of the activity of BCMS compliance with ISO 22301:2012 and expectations of management. It also seeks feedback from management regarding expectations.
- Section 10 is an element of "action". It identifies the actions of non-compliance in BCMS through corrective action.

Requirements for risk assessment ISO 9001:2008 and ISO 22301:2012

Risk assessment is an essential element of business continuity management. Risk assessment is also a critical element of business continuity or political processes that is essential for the organization. Risk assessment of business processes is essential for quality management according to ISO 9001:2008, for products and services offered by the organization. In those standards, as well as all versions of ISO 9001 before there is no requirement for a risk assessment process. Considering the importance of this issue in the period 2009 - 2013 ISO published series of ISO 31000 standards:

- ISO 31000:2009 "Risk Management. Principles and guidelines";
- ISO/TR 31004:2013 "Risk Management. Guidelines for the implementation of ISO 31000";
- ISO 31010:2009 "Risk Management. Methods of risk assessment."

Getting acquainted with the texts of the above-mentioned standards stakeholders can see that the risk assessment is an element of its management. Its ultimate objective is to maintain the original measured level of risk or reduce it to an acceptable level, or its removal. The ISO 31000:2009 does not require certification implemented MS risk. It should be noted comic circumstance that with the release of this standard part of organizations in Bulgaria "rushed" to seek ways to be ISO 31000 certified. These organizations expected in public procurement to appear requirement of an ISO 31000:2009 certifications. Such requirements are not set and after about a year of the publication of the standard interest in Bulgaria towards the introduction of MS of risk declined. Unfortunately, we have no understanding that risk management is a universal mechanism for successful and reliable operation (continuous processes) of all MS according to the requirements of the ISO-standards. It should be noted that the MS of risk are also applicable in standards related to conformity assessment (such as ISO/IEC17021:2011, ISO/IEC 17020:2012, ISO/IEC 17025:2005 and others), which are subject to confirmation by the Executive Agency "Bulgarian Accreditation Service".

Considering the importance of risk to maintain continuity of business and political processes, ISO 22301:2012 explicitly requires risk assessment. Below the text of item 8.2.3 "Risk assessment" is quoted.

The organization shall establish, implement, and maintain a formal documented risk assessment process that systematically identifies, analyses, and evaluates the risk of disruptive incidents to the organization.

NOTE This process could be made in accordance with ISO 31000.

The organization shall

a) Identify risks of disruption to the organization's prioritized activities and the processes, systems, information, people, assets; outsource partners and other resources that support them,

b) Systematically analyze risk,

c) Evaluate which disruption related risks require treatment, and

d) Identify treatments commensurate with business continuity objectives and in accordance with the organization's risk appetite.

NOTE: The organization must be aware that certain financial or governmental obligations require the communication of these risks at varying levels of detail. In addition, certain societal needs can also warrant sharing of this information at an appropriate level of detail.

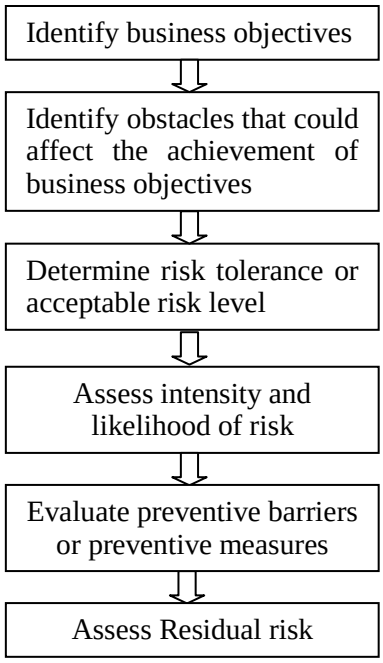
As seen in the above text, as well as in that bibliography of ISO 22301:2012, the risk management and control systems business continuity is also based on the ISO 31000 series.

ISO 31000 offers suggestions and variety of risk assessment methodologies. Some of them are more industry specific, but some a universally applicable.

Performing business risk assessment requires defining and consistently applying an approach that is approved by the organization. Any risk assessment should include scope and plan, objectives, responsibilities, timelines, and input and output requirements. Some organizations use Suppliers, Input, Process, and Output and Customers (SIPOC) approach to determine input and output requirements.

Sources of input are determined based on available information like lessons learned from business losses. Output requirements are derived based on the specific management and business partner's requirements.

Once the scope and plan of the risk assessment are developed, the risk assessment process should include the following six steps:



A simple risk assessment matrix can be used business risk assessments. An example of risk assessment matrix used for occupational health and safety (OSH) assessment is provided in ANSI Z590.3. 2011 Prevention through Design standard. Similar matrix can be used to provide semi-quantitative business risk assessment evaluation. We can demonstrate the use of such business risk assessments with the following practical example.

On October 2, 2014, explosions wrecked the Midzhur plant in Gorni Lom, Bulgaria. According to NY Times, the explosions were so powerful that they annihilated the factory, leaving behind little but two yawning craters.

(Ref:http://www.nytimes.com/2014/10/03/world/europe/deadly-blasts-in-bulgaria-rip-through-plant-decommissioning-land-mines.html?_r=0)

It is unclear if the factory management had proper business risk assessment. However, it is clear that the business continuity risk from a potential explosion is enormous. Two previous explosions at the Midzhur plant, in 2007 and 2010, injured six people, and two buildings were flattened in the 2010 blast. (Same ref. as above) Therefore, applying the business risk assessment methodology would have produced the following results.

PTD BC

Assess Business Risk Associated with Explosion Hazard

Business Risk Assessment Matrix: Numerical Ratings

Risk of business continuity loss from Hazardous Work Environment

Outcomes	Explosion	Financial	Ethical	Legal
Intensity Rating:	5	4	4	5
Likelihood Rating:	4	4	3	4
Total		16	12	20

		Likelihood of Business Losses				
RA Matrix		5	4	3	2	1
Extent of Impact	5	25	20	15	10	5
	4	20	16	12	8	4
	3	15	12	9	6	3
	2	10	8	6	4	2
	1	5	4	3	2	1

Where: Severity or Intensity effect on the business will be ranked at 5 (Catastrophic) and the Likelihood will be ranked at 4 (Likely), based on previous experience. Semi quantitative ratings are based on the following scales.

Incident or Exposure Severity Descriptions

5. Catastrophic: One or more fatalities, total system loss, chemical release with lasting environmental or public health impact.

4. Critical: Disabling injury or illness, major property damage and business downtime, chemical release with temporary environmental or public health impact.

3. Marginal: Medical treatment or restricted work, minor subsystem loss or damage, chemical release triggering external reporting requirements.

2. Negligible: First aid or minor medical treatment only, non-serious equipment or facility damage, chemical release requiring routine cleanup without reporting.

1. Insignificant: Inconsequential with respect to injuries or illnesses, system loss or downtime, or environmental chemical release.

Incident or Exposure Probability Descriptions

1. Unlikely: Improbable, may assume incident or exposure will not occur.
2. Seldom: Could occur, but hardly ever.
3. Occasional: Could occur intermittently.
4. Likely: Probably will occur several times.
5. Frequent: Likely to occur repeatedly.

As a next step, we can evaluate the business impact using similar risk assessment rankings. However, Severity rating is replaced with Extent of Impact on business and Probability rating is replaced with Likelihood of Business Losses. An example of three business categories risk assessment is presented below.

Extent of Business Losses Impact Descriptions

1. Insignificant: Inconsequential with respect to business losses.
2. Negligible: Minor business losses.
3. Marginal: Business losses triggering external reporting requirements.
4. Critical: Business downtime, significant business losses or corporate image impact.
5. Catastrophic: Unsustainable losses, total business loss, inability to continue business operations.

Likelihood of Business Losses Descriptions

1. Unlikely: Improbable, may assume business loss will not occur.
2. Seldom: Could occur, but hardly ever.
3. Occasional: Could occur intermittently.
4. Likely: Likely to occur several times.
5. Frequent: Likely to occur repeatedly.

If the company eliminates the high explosive ammunitions destruction practices, and decides to strictly enforce safety procedures, the same business risk assessment matrix could be used to re-evaluate the risk. In this case, we are going to use at least three Layers of Protection:

1. Elimination of high explosive ammunitions dismantling practices.
2. New safety procedures
3. Safety training

In this case, more likely will see the following results.

PTD BC

Assess Business Risk with Proposed Intervention

Business Risk Assessment Matrix: Numerical Ratings

Risk of business continuity loss

Outcomes	Explosion	Financial	Ethical	Legal
Intensity Rating:	4	3	2	1
Likelihood Rating:	2	2	2	2
Total		6	4	2

RA Matrix		Likelihood of Business Losses				
		5	4	3	2	1
Extent of Impact	5	25	20	15	10	5
	4	20	16	12	8	4
	3	15	12	9	6	3
	2	10	8	6	4	2
	1	5	4	3	2	1

The last step of the business risk model is to assess the residual risk. The authors suggest using the percentage reduction. Business risk reduction calculation shows 75% risk reduction. That is considered significant reduction and should be acceptable to the management of the company. Business risk reduction calculations are presented below.

BUSINESS RISK REDUCTION

	Business losses from hazardous work environment	Risk Factor CS	Risk Factor FS	% Risk Reduction	% Residual Risk
	Financial	16	6	62.50%	37.50%
	Ethical	12	4	66.67%	33.33%
	Legal	20	2	90.00%	10.00%
	Total	48	12	75.00%	25.00%
Is this an acceptable level of Business Risk?			Yes		

The business risk assessment model presented above is just one of the risk assessment methodologies described in ISO 31010 and American Prevention through Design standard. There are at least twenty two other risk assessment methodologies described in ISO 31000 standards.

CONCLUSIONS

An attempt was made to show the some of the tools that support the practical application of ISO 22301:2012. The authors do not believe that these are the only tools for business continuity. Many other risk assessment tools are presented in ISO 31010. At the request of the adopters of the standard, other methods for risk assessment, shown in ISO 31010, can be developed.

In conclusion, the authors would like to inform the interested parties that we will continue to create other practical tools supporting the implementation of ISO 22301:2012. Such tools are recommended in ISO 22514 series of standards dealing with statistical measurement of the processes.

REFERENCES

1. ISO 22301:2012 „Societal security. Business continuity management systems. Requirements“.
2. ISO/IEC17021:2011 „Conformity assessment. Requirements for bodies providing audit and certification of management systems“.
3. ISO/IEC 17020:2012 „Conformity assessment. Requirements for the operation of various types of bodies performing inspection“.
4. ISO/IEC 17025:2005 „General requirements for the competence of testing and calibration laboratories“.
5. ISO 31000:2009 "Risk Management. Principles and guidelines ";
6. ISO/TR 31004:2013 "Risk Management. Guidelines for the implementation of ISO 31000 ";
7. ISO 31010:2009 "Risk Management. Methods of risk assessment“.
8. ISO 22514 „Statistical methods in process management“.