VIII INTERNATIONAL CONFERENCE

QUALITY SYSTEM CONDITION FOR SUCCESSFUL BUSINESS AND COMPETITIVENESS

PROCEEDINGS

ASSOCIATION FOR QUALITY AND STANDARDIZATION OF SERBIA

25.11.-27.11.2020

ASSOCIATION FOR QUALITY AND STANDARDIZATION OF SERBIA

VIII INTERNATIONAL SCIENTIFIC CONFERENCE

QUALITY SYSTEM CONDITION FOR SUCCESSFUL BUSINESS AND COMPETITIVENESS

PROCEEDINGS

25/11 – 27/11/2020

Organizer

ASSOCIATION FOR QUALITY AND STANDARDIZATION OF SERBIA
e-mail: office@aqss.rs
web: www.aqss.rs

CO-ORGANIZER

FACULTY OF VETERINARY MEDICINE UNIVERSITY OF BELGRADE
web: www.vet.bg.ac.rs

IN COOPERATION WITH

CENTER FOR QUALITY FACULTY OF MECHANICAL ENGINEERING IN KRAGUJEVAC
web: www.cqm.rs
e-mail: cqm@kg.ac.rs

CENTER FOR QUALITY OF FACULTY OF MECHANICAL ENGINEERING PODGORICA
web: www.cq.ac.me
e-mail: centerforquality@ac.me

Академија струковних студија Шумадија

SHUMADIA ACADEMY OF PROFESSIONAL STUDIES

Web: www.asss.edu.rs
e-mail: office@asss.edu.rs

MIDDLE AND SOUTHEASTERN EUROPE QUALITY INITIATIVE
e-mail: miroslav.drljaca1@zg.t-com.hr
web: www.hdmk.hr

with support

Republic of Serbia
Ministry of Economy
www.privreda.gov.rs

Accreditation body of Serbia
www.ats.rs

Serbian Association of Employers
www.poslodavci.rs

Institute for standardization of Serbia
www.iss.rs

PROCEEDINGS

Publisher:

Association for quality and standardization of Serbia

For publisher :

Professor Zoran Punoševac PhD

Editorial board:

Professor Zoran Punoševac PhD

MSc. Ana Jelenković

Ivan Vesić

Print:

SaTCIP d.o.o ,Vrnjačka Banja

No. of copies :

50

ISBN 978-86-80164-15-1

SCIENTIFIC COMMITTEE

Prof. Zoran Punoševac Ph.D.(Serbia) - president
Prof. Slavko Arsovski Ph.D.(Serbia)
Prof. Vlado Teodorović Ph.D (Serbia)
Prof. Zdravko Krivokapić Ph.D.(Crna Gora)
Prof. Slavisa Moljevic PhD (Bosnia and Herzegovina)
prof. Miladin Stefanovic Ph.D (Serbia)
Prof. Milan J. Perović Ph.D.(Crna Gora)
Prof. Aco Janićijević Ph.D.(Serbia)
Prof. Radomir Radovanović Ph.D. (Serbia)
Prof. Dušan Cogoljević Ph.D (Serbia)
Prof. Adolfo Senatore Ph.D. (Italy)
Prof. Aleksandar A. Boljsakov Ph.D. (Russia)
Prof. Ani P. Petkova Ph.D.(Russia)
Prof. Carol Zoller Ph.D.(Romania)
Prof. Jozef Peterka Ph.D. (Slovakia)
Sc Miroslav Drljača Ph.D. (Croatia)
Prof. Krešimir Buntak Ph.D. (Croatia)
Prof. Stanislav Borkovski Ph.D.(Poland)
Prof. Marianna Kazimierska-Grebosz Ph.D. (Poland)
Prof. Nikolaos Vaxevanidis Ph.D.(Greece)
Sc Dobrila Jakić Dimić Ph.D.(Serbia)
Prof. Dragan Šefer Ph.D (Serbia)
Assoc. Prof. Raycho Ilarionov Ph.D.(Bulgaria)
Prof. Valentin Nedeff Ph.D.(Romania)
Prof.dr Viktor Vladimirovic Timcenko Ph.D.(Rusija)
Prof.ing Jiri Plura Csc (Czech)
Prof.Larisa Gromova Ph.D. (Russia)
Prof. Vladimir A. Fedorinov Ph.D.(Ukraine)
prof. Elizabeta Mitreva, Ph.D.(North Macedonia)

ORGANIZING COMMITTEE

Prof.dr Zoran Punoševac Ph.D., president
Prof. Danijela Kirovski Ph.D
Ana Jelenković, secretary
Ivan Vesić
Miloš Punoševac

PREFACE

Dear Colleagues, Ladies and Gentlemen,

I take great pleasure in welcoming you to the 22nd National and 8th International Scientific Conference on QUALITY SYSTEM CONDITION FOR SUCCESSFUL BUSINESS AND COMPETITIVENESS, organized by the Association for Quality and Standardization of Serbia.

In the past period, we have successfully organized 21 national and 7 international quality conferences where a large number of papers were published, with a large number of authors and co-authors and most importantly, with a large number of participants

This year, the organization of the conference got a completely different character due to the COVID-19 pandemic, so we organized the On line conference. The decision on the manner in which the conference will be organized was made only 15 days before the event, bearing in mind that at that time Government made a regulation to ban gatherings of more than 5 people indoors (in this case in the conference hall).

This year we are organizing the 22nd National and 8th International Scientific Conference in cooperation with:

- *Faculty of Veterinary Medicine, Belgrade University – co-organizer*
- *Quality Centre, Faculty of Engineering Sciences, Kragujevac University*
- *Quality Centre, Faculty of Mechanical Engineering, University of Montenegro, Podgorica*
- *Middle and South East European Countries Quality Initiative*
- *Shumadia Academy of professional studies,*

with the support of

- *Ministry of Economy of the Republic of Serbia*
- *Accreditation Body of Serbia*
- *Serbian Association of Employers*
- *Institute for Standardization of Serbia*

The sponsor of the conference is Trayal Corporation from Kruševac

A number of papers have been submitted for this conference, which have been published in this proceedings, but the emphasis is on round tables, which are expected to be attended by a larger number of participants.

- *THE FUTURE OF REMOTE AUDIT where the current practice and future directions of development of these new audit methods and techniques of verification would be pointed out.*
- *CORONAVIRUS PANDEMIC AND CRISIS MANAGEMENT, with the main goal of understanding the aspects of crisis management in the context of a coronavirus pandemic, as well as the consequences of the pandemic on the economic and financial system*
- *FOOD SUPPLY CHAIN IN THE CONDITIONS OF THE COVID-19 PANDEMIC, which will discuss the global food crisis in the world and its consequences, which were further deepened in 2020 by the SARS-Cov-2 pandemic (Covid-19) and finding possible solutions for the period ahead*
- *FUTURE CONCEPTS OF STANDARDS FOR MANAGEMENT SYSTEMS with the aim of presenting the future concept of development of the ISO 9001 series of standards bearing in mind that the draft future concept of standards for management systems provides framework topics to be addressed in the future by ISO 9000 series standards and organizations applying standards for management systems.*

This year, as well as every subsequent year, we will give recognition to those who have contributed to the success of the conference.

This year, as every next year, we will award prizes to deserving members for their contribution to the work of the Association as well as to the improvement of the quality infrastructure in Serbia

The success of a conference depends on all the participants, therefore, I take the opportunity to thank all the authors and co-authors of the papers, the co-organizer, the general sponsor, other sponsors and donors, media patrons, as well as all the participants from Serbia and abroad.

I would like to wish us successful work and a good time at the largest gathering devoted to quality.

Yours sincerely,

Professor Zoran Punoševac, PhD
Organizing Committee Chairman

CONTENTS

ASSOCIATION FOR QUALITY AND STANDARDIZATION OF SERBIA
22nd national and 8th international conference
QUALITY SYSTEM CONDITION FOR SUCCESSFUL BUSINESS AND COMPETITIVENESS

METHODOLOGICAL APPROACH ENSURING BUISNIUES CONTINUITY BASED ON INFORMATIONAL RISK ASSESSMENT

Matija Kovačić, mag.ing.traff[1]

prof.dr.sc. Krešimir Buntak[2]

Ernest Forjan, bacc.oec.[3]

Abstract: *Whit increasing turbulency in the organizational environment, there is an increasing challenge related to creating and ensuring business continuity of the organization. One of the especially important areas that determine business continuity is information security. Information security is particularly endangered because of the digitalization of the business system and digital transformation. One of the risks that are related to the digital transformation and translation of the business to the digital sphere is the threat of access to information from third parties that may misuse such information. Accordingly, there is a need for creating a conceptual model for ensuring the security of the information in the organization as well as the way of creating businesses continuity plans*

Keywords: *bussniues continuity, risk approach, cortporative seafty, information seafty;*

JEL Klasifikacija*: L21*

1. INTRODUCTION

Whit the development of Industry 4.0 there is a need for all organizations to conduct digital transformation. Digital transformation for the organization means the possibility of increasing efficiency and effectiveness but on the other hand, there is also a challenge that is related to the managing of new risks that are arising through the usage of new technology. One of the most pronounced risks is an informational risk that is related to the leaking of information to the public or risk that third parties can access organizational information. Whit arising risk of information security as well as the endangering organizational information there is also a risk of endangering

[1] Matija Kovačić, mag.ing.traff., University North, Koprivnica, Croatia, matkovacic@unin.hr
[2] Prof.dr.sc. Krešimir Buntak, University North, Koprivnica, Croatia, krbuntak@unin.hr
[3] Ernest Forijan, bacc.oec., University North, Koprivnica, Croatia, erforjan@unin.hr

organizational corporative safety.[4] Information risk is endangering corporative safety because corporative safety is made from different kinds of fields and one of the fields is an information security and risk management. So, whit endangering information security there is also an increased risk of endangering corporative safety which can lead to the decreasing possibility of the organization to continue doing business. In other words, corporative safety determines the business continuity of the organization because the information that are stored in the organization are important for normal functioning of the organization.[5] Furthermore, digitalization also means translation specific information that is stored in physical documents in the organization to the cloud and virtual sphere. Virtualization and digitalization of the information create a new risk that is related to the possibility of leaking such information to the public. There is also a risk of cyber-attacks that will as the result have stolen information or publishing some of the information to the public. To decrease such risks, an organization must create and conduct a risk assessment. Furthermore, after risk assessment, the organization must create plans for ensuring business continuity as well as the plan for increasing corporative safety. Every risk that an organization identifies must be analyzed and for every risk, an organization must create measures for decreasing identified risk. This approach results in increasing corporate safety. There is also a risk that business secrets that organizations have and it is related to the business models can leak to the public and also endanger business continuity.[6] Whit increasing the importance of the information that is stored in the organization, as well as the increasing of the vulnerability of the information that is the risk of disruption of business continuity higher. Because of that, the organization must conduct risk assessment whit different kinds of methods and tools that are described in different kinds of norms such as ISO EN 30001:2018 and ISO/IEC 31010:20019. Furthermore, there is also a need for the creation of the concept that will help the organization in creating plans based on conducted risk assessment.

The main aim of this paper is to create a methodological approach that will become one of the steps in creating business continuity plans. Furthermore, the aim of this paper is also to shown importance of the information security and its relations to the business continuity and competitive advantage of the organization.

2. RISK AND IMPACT OF RISK ON THE BUSINESS

Risk as such can be defined as the impact of the insecurity on the goals. In other words, the development of risk can impact the achieving of defined goals in the organizational plans.[7] Impossibility of the organization of achievement its own goals can result in a decrease in the effectiveness and efficiency of the organization because efficiency is related to the resources that an organization must invest in the process of achieving goals. So, decreasing inefficiency is leading to a decreasing in effectiveness because organizations do not achieve planned goals related to the using of resources. The impact of the risk to the organization is determined whit the type of risk.

Risk can be divided into:

- Financial risk: financial risks are related to the uncertainty of financing as well as the changes in financial markets that can significantly impact the ability of the organization to achieve goals. Some of the examples of the financial risks are changes in the interest rates, changes in the availability of financial resources, etc.

---

[4] Wijnia, Y., & Nikolic, I. (2007). Assessing business continuity risks in IT. *IEEE International Conference on Systems, Man and Cybernetics*, str. 3547-3553.

[5] Cioc, M., & Ursacescu, M. (2012). Information systems'risk management–an empirical research in romanian companies. *AMIS*.

[6] Vlachos, T. (2018). Certifiable Risk Management & Business Continuity approach in mining industry. *World Congress on Mechanical, Chemical, and Material Engineering*.

[7] Renault, B. Y., Agumba, J. N., & Ansary, N. (2016). A theoretical review of risk identification: perspective of construction industry. *ARCA*, str. 773-782.

- Infrastructure risks: infrastructure risk is related to all events that can impact infrastructure such as the disruption in the telecommunication infrastructure, natural disasters that can impact infrastructure and possibility of using infrastructure for organization needs,
- Market risks: market risks are related to the market trends and developments on the market such as economic crisis, competition moves that can result in developing crisis in the organization or decreasing demand for the goods and services,
- Reputation risk: that is related to the corporate social responsibility, perception of the buyers that are building based on the decision of the management. [8]

Risks have a fundamental property that is related to the impossibility of their prediction. In other words, the uncertainty of risk is related to the impossibility of the organization to assess all risks as well as the possibility to analyze all risks for all sources. [9] That impossibility in first place sources from large financial resources that the organization must invest in the risk assessment and creating measures for decreasing risk. Furthermore, impossibility is related also to the unpredictability of the organizational environment. Changes in the organizational environment can lead to the development of the new risks than can as the result have to endanger organizational business continuity or competitiveness.

Risks have a high impact on the entire organization as well as all functions and departments in the organization. They can lead to the creating of costs because of the need for remediation of consequences of the development risk. Because of the areas from which risk can be developed such as the management, human resources, market, etc., there is a need and imperative for risk assessment and developing measures for decreasing identified risk to prevent disruption of the business continuity.

It should be highlighted that impact of the risk on the organization is determined through the resistance of the organization. Whit the increasing resistance that is related to the possibility of an organization dealing whit crisis and risk, that is the impact of the risk on the organization smaller. Furthermore, increasing of the organizational resistance is determined through corporative safety because corporative safety encompasses almost all risks and areas from which risk can arise.[10]

2.1. Information risks

Information risk may be related to the unauthorized access to the information that is stored in different databases as well as they are documented in the organization. Such databases may be protected in different ways such as protection whit usage of firewall that is protecting data from unauthorized access. Furthermore, databases that are used for the storage of the organizational information can be protected whit different encryption techniques. Such encryption techniques are used for the coding of information so third parties cannot access or understand encrypted data. When encrypted, information must be decrypted whit special software. Such software can be implemented in the computer systems in the organization and only computers that have such software can show information that is encrypted. This kind of encryption is often used in a financial organization to protect customer data and transactions from the costumers.[11] Depend on data and its sensitivity depends the encryption technique that is used for encryption. So, there is a significant difference between encryption techniques that are used to protect cells or the entire database. Furthermore, the encryption technique that will be used for the protection of data is determined whit programing language that is used for the programming database.

[8] Živko, I., Marijanović, Z., & Grbavac, J. (2015). Rizici u poslovanju - Upravljanje pristupom financija i računovodstva. *Zbornik radova Ekonomskog fakulteta Sveučilišta u Mostaru, No. Posebno izdanje 2015*, str. 401-412.
[9] Toma, S. V., Chiriță, M., & Șarpe, D. (2012). Risk and uncertainty. *Procedia Economics and Finance*, str. 975-980.
[10] Vogus, T. J., & Sutcliffe, K. M. (2007). Organizational resilience: towards a theory and research agenda. *IEEE International Conference on Systems, Man and Cybernetics* , str. 3418-3422.
[11] Sesay, S., Yang, Z., Chen, J., & Xu, D. (2005). A secure database encryption scheme. *Second IEEE Consumer Communications and Networking Conference*, str. 49-53.

Except for unauthorized usage of data stored in the database, there is also a list of different kinds of risks that are related to the information that is documented in offices in the organization. Employees that do not have authorization for access such information can through insight in the document and its content endanger business secret and all other information that are related to the organization and way of doing business. Besides, one of the most significant risks is cyber-attacks that can be performed by third parties. Cyber-attacks can endanger information that organizations have and can endanger the business continuity of the organization. Such information may be related to the data of employees, data of costumer, etc.[12] It should be highlighted that there is also a possibility for the organization employees, because they may be malicious, to seek for the protected data and to forward such data to the third parties and whit that endanger organization business continuity.

2. BUSINESS CONTINUITY MANAGEMENT

Business continuity management is a process of development plans and defining measures that will be aimed at creating a strategy for continuing of doing business after incidents occur and to ensure the safety of the organization. [13] In other words, business continuity management is based on prevention and its aimed at the timely identification of risks to avoid interruption of the business continuity.

Business continuity management consists of activities such as risk management, crisis management, and all other activities that can disrupt business continuity. Furthermore, business continuity management is based on different kinds of plans:

- Recovery plan: in recovery plan organization is defining and allocating all resources that are needed for recovering business after occurring an incident or other unwanted event. In other words, the recovery plan may within it consist of procedures that will be activated after an incident occurs, and is aimed at the communication whit different stakeholders, etc.,
- Response to an incident plan: this kind of plan consists of procedures that must be activated to decrease the impact of the incident on the organization activities. So, this plan consists of different kinds of standard operating procedures that are activated after the incident has occurred in the organization.[14]

The core business of the organization determinate recovery plan and also a business continuity plan. Organizations like healthcare organizations that are especially important for normal functioning of the society must have developed plans that will ensure business continuity management because interruptions in the activities of such organizations can as result have the decreasing quality of life of all society as well as the occurring different kind of new diseases.

When it comes to the business continuity management and recovery plans, it should be highlighted that the recovery plan as well as the business continuity plan must be implemented in the organizational processes through procedures. Whit procedures can be defined what activities will be activated if there is a treat of interruption of the business. Furthermore, when it comes to business continuity management, it should be highlighted that there is also a need for implementing measures for ensuring the safety of the information. Within defined procedures, organizations must define measures that will take place if there is a risk of endangering organizational information.

[12] Sek Seong Lim, M. (2017). Business Continuity Management and Cybersecurity. *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, str. 185-192.
[13] Costello, T. (2012). Business continuity: Beyond disaster recovery. *IT Professional*, str. 64-64.
[14] Herbane, B., Elliott, D., & Swartz, E. M. (2004). Business continuity management: time for a strategic role? *Long Range Planning*, str. 435-457.

3. CORPORATIVE SAFETY

Corporative safety is related to the care of the different areas within the organization as well as the performing different kind of activities that are aimed at increasing safety in the organization.15 In other words, corporative safety within it consists of different kind of activities such as:

- Fire protection: that is related to the planning of measures related to the fire extinguishing as well as the ensuring normal functioning of the equipment that is used for the fire extinguishing,
- Protection of property and people: that is related to the protection of people that are working in the organization as well as the technical protection such as installing a different kind of security cameras to protect the property of the organization,
- Safety at work: that is aimed at protection and prevention of injury that employees can suffer when they performing their activities. Furthermore, implies also to the education of all employees for performing activities on safety way,
- Data protection: is related to the analyzing of risk related to the possibility of leaking information from the organization and unauthorized access of third parties to the organization information,
- Business intelligence: is related to the intelligence work related to the market and environment in which organizations exist. Furthermore, business intelligence is related to the analysis of data as well as all information that can be used by the organizational competition in the market and also protect the usage of information by the employees that are not authorized for it.

Within corporative safety, information security has a special role because information has an important role in the normal functioning of the organization. Information safety is related to the all information and data that are stored in the organization and that are related to the organizational employees, business results, plans of the organization, risks that may treat organization, information about suppliers, etc. Furthermore, one of the most important areas of corporate security is intellectual property. Intellectual property is related to the new patents and innovations that are developed by organizational employees and such innovations may become one of the competitive advantages of the organization.

3.1. Informational security

When it comes to the information security it should be highlighted that informational security is in the Republic of Croatia determined whit legislative such as:

- Law of protection of personal data,
- Law of informational security,
- Law of security of data,
- Law of the electronic document,
- Law on the Security and Intelligence System of the Republic of Croatia

All mentioned lows are base for the normal functioning of the system of protection of information in every system besides if is a business system or all other types of the system. Furthermore, besides Laws, an organization can implement norms such as ISO EN 27001:2018 norm that shapes the information security management system.

Furthermore, informational security in an organization is related to the protection of all information that is related to the organizational employees, patents, innovations, dana related to the suppliers

[15] Huang, Y. H., Chen, P. Y., Krauss, A. D., & Rogers, D. A. (2004). Quality of the execution of corporate safety policies and employee safety outcomes: assessing the moderating role of supervisor safety support and the mediating role of employee safety control. *Journal of Business and Psychology*, str. 483-506.

and buyers, etc. It should be highlighted that informational security is determined through different kinds of elements of corporative security such as business intelligence, technical protection, etc.[16]

4. METHODOLOGICAL APPROACH ENSURING BUISNIUES CONTINUITY BASED ON INFORMATIONAL RISK ASSESSMENT

Since organizational exists in the environment that is turbulent, fast changes in the environment as a result have new risks. New risks in a significant way can endanger business continuity of the organization as well as corporative safety if the organization on time does not identify risks and create measures for risk decreasing and decreasing consequence of the risk. In other words, risks can endanger the continuity of the organization that can be determined whit corporative safety. Furthermore, one of the most important components that can determine the business continuity of the organization is information safety. The information system of the organization meets different kinds of risks and challenges because of digital transformation and virtualization of the data. Whit digitalization of the data, data can be easily accessed through Internet so third parties that can be malicious can access and stole dana stored in the databases. Furthermore, there is also the risk of cyber-attacks that can be also aimed at the misusage of the information. Accordingly, it is necessary to identify all risks that could endanger information that is stored in the databases in the organization as well as all documents that are stored in offices in the organization that could be endangered by unauthorized views.

One of the ways for dealing whit risks and ensuring business continuity is implementing the business continuity management system and to certificate it whit norm ISO EN 22301:2019 as well as the implement risk management system that is shaped through ISO EN 31000:2018. It should be highlighted that implementing such a system is only a base for ensuring business continuity of the organization and organizations must ensure also different kinds of activities that will support such systems i.e. provide risk assessments, etc.

All changes in the market must be accompanied by a whit new risk assessment. In other words, risk management is a continuous process that is made in different iterations. The time within which the organization will repeat risk assessment related to the new condition in the market depends on the type of business that takes place in the organization as well as on the decision of management. Furthermore, how the organization will deal whit risk depends on the risk policy and policy of ensuring business continuity that is created by the management of the organization.[17] Accordingly, Figure 1 shown steps when an organization is creating plans for ensuring business continuity. As shown in Figure 1, the first step is risk analysis. Organizations must analyze all risks that can appear from organizational environments such as the internal environment and general environment. In other words, organizations analyze risk through the frequency of risk, high impact, and high consequences. Organizations should analyze such risk whit methods such as FMEA that is an acronym for Failure Mode and Effects Analysis. FMEA method is based on the analysis of the area from which risk can appear. After defining area, all risks that can appear are identified and for each risk is analyzed the impact of the risk, consequences of the risk as well as the frequency of the risk. This is based on the creating measures and procedures that will be activated if an incident occurs. Furthermore, if information safety is considered, an organization must analyze all risks that can endanger the safety of the information. Also, the organization can perform penetration tests related to the possibility of third parties to penetrate databases and to steal information from it.

Except for penetration tests of databases, it is necessary to analyze the possibility that third parties could access information that is stored in offices in the organization. Such information can be stored

[16] Mishra, S., & Chasalow, L. (2011). Information security effectiveness: A research framework. *Issues in Information Systems*, str. 246-255.

[17] Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, str. 1-13.

in offices and different parties could access information and steal it. Furthermore, it is also recommended to test the possibility of eavesdropping as well as usage telecommunication equipment for the personal purpose of the employees. Such behavior can result in the misusage of the equipment and the possibility of leaking information. Furthermore, an organization can test the possibility of the organizational employees to copy files that are stored on their computers and to take that information to the house.

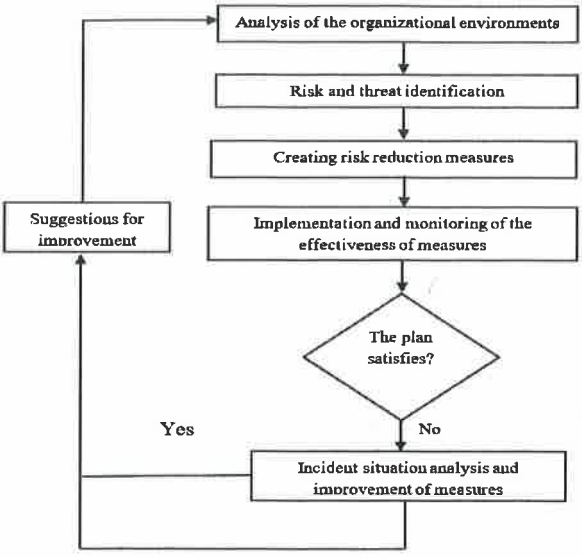

Figure 1. Diagram flow of the creating information security and business continuity plan

Source: Author work

After the organization identifies threats and weaknesses, it should define measures that will be used for risk reduction and decreasing risk of information leaking. Such measures must be implemented in the organizational plan of ensuring business continuity as well as the plan for ensuring corporative safety because of the fact that such a plan consists of different kinds of areas such as informational safety, fire protection, etc. After defining measures, an organization must conduct tests for identifying efficiency and effectiveness of created measures as well as the education of the employees so employees will be in the possibility to answer if in the organization occurs incident.

One of the recommendations when it comes to ensuring business continuity is to implement a process approach and to defined so-called KPI (Key Performance Indicators) that will be used for the tracking indicators of informational safety. KPIs can be implemented in the processes where is a possibility and risk for unauthorized access to the information. These kinds of indicators must be included in the business continuity plans as well as the plans for ensuring corporative safety.

If an incident occurs in the organization that is related to the informational security, it is necessary to analyze the root cause of the incident as well as to conduct all measures that will decrease the consequences of the incidents. Furthermore, the organization must define measures to prevent the occurrence of such risks in the future and such measures must be implemented to the new plans.

5. CONCLUSION

This paper is describing the methodological approach to ensuring business continuity based on ensuring informational safety and risk assessment. It should be highlighted that the development of the informational safety plan as well as the corporative safety plan is part of creating a business continuity strategy. In other words, the organization must repeat analysis for all segments of the business and then integrate them into one plan.

Corporative safety is based on creating a business continuity plan for the organization. For creating such a plan, the organization must conduct a risk assessment as well as provide analysis of all areas that can be affected by whit the risks. Whit the identification of those areas it is necessary to define measures for the decreasing of the risk as well as to conduct the education of the organizational employees.

Through the digitalization of the organization and an increasing number of risks that are arising from changes in organizational environments, the organization must pay special attention to informational security. Informational security is related to all information that is stored within the organization and is related to all types of misusage of the information that can come from organizational employees as well as third parties.

LITERATURE

[1] Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. European Journal of Operational Research, str. 1-13.

[2] Cioc, M., & Ursacescu, M. (2012). Information systems'risk management–an empirical research in romanian companies. AMIS.

[3] Costello, T. (2012). Business continuity: Beyond disaster recovery. IT Professional, str. 64-64.

[4] Herbane, B., Elliott, D., & Swartz, E. M. (2004). Business continuity management: time for a strategic role? Long Range Planning, str. 435-457.

[5] Huang, Y. H., Chen, P. Y., Krauss, A. D., & Rogers, D. A. (2004). Quality of the execution of corporate safety policies and employee safety outcomes: assessing the moderating role of supervisor safety support and the mediating role of employee safety control. Journal of Business and Psychology, str. 483-506.

[6] Mishra, S., & Chasalow, L. (2011). Information security effectiveness: A research framework. Issues in Information Systems, str. 246-255.

[7] Renault, B. Y., Agumba, J. N., & Ansary, N. (2016). A theoretical review of risk identification: perspective of construction industry. ARCA, str. 773-782.

[8] Sek Seong Lim, M. (2017). Business Continuity Management and Cybersecurity. The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities, str. 185-192.

[9] Sesay, S., Yang, Z., Chen, J., & Xu, D. (2005). A secure database encryption scheme. Second IEEE Consumer Communications and Networking Conference, str. 49-53.

[10] Toma, S. V., Chiriță, M., & Șarpe, D. (2012). Risk and uncertainty. Procedia Economics and Finance, str. 975-980.

[11] Vlachos, T. (2018). Certifiable Risk Management & Business Continuity approach in mining industry. World Congress on Mechanical, Chemical, and Material Engineering.

[12] Vogus, T. J., & Sutcliffe, K. M. (2007). Organizational resilience: towards a theory and research agenda. IEEE International Conference on Systems, Man and Cybernetics , str. 3418-3422.

[13] Wijnia, Y., & Nikolic, I. (2007). Assessing business continuity risks in IT. IEEE International Conference on Systems, Man and Cybernetics, str. 3547-3553.

[14] Živko, I., Marijanović, Z., & Grbavac, J. (2015). Rizici u poslovanju - Upravljanje pristupom financija i računovodstva. Zbornik radova Ekonomskog fakulteta Sveučilišta u Mostaru, No. Posebno izdanje 2015, str. 401-412.

CIP - Каталогизација у публикацији

Народна библиотека Србије, Београд

005.6 (082)

005.334 (082)

005 (082)

INTERNATIONAL scientific conference Quality system condition for successful business and competitiveness (8 ; 2020)

Proceedings / VIII International scientific conference Quality system condition for successful business and competitiveness, 25/11 - 27/11/2020 ;

[organizers] Association for quality and standardization of Serbia ... [et al.] ; [editorial board Zoran Punoševac, Ana Jelenković, Ivan Vesić].

- Kruševac : Association for quality and standardization of Serbia, 2021 (Vrnjačka Banja : SaTCIP).

- 62 str. : graf. prikazi, tabele ; 25 cm

"... On line conference..." --> preface. - Tiraž 50. - Str. 6-7: Preface / Zoran Punoševac. - Napomene i bibliografske reference uz tekst. - Bibliografija uz svaki rad..

ISBN 978-86-80164-15-1

1. Punoševac, Zoran, 1956- [уредник] [аутор додатног текста]

а) Управљање квалитетом -- Зборници

б) Менаџмент -- Зборници

в) Управљање ризиком -- Зборници

COBISS.SR-ID 31979785