

E-business Continuity Management in Insurance Sector

Milica Labus*

*University of Belgrade, Faculty of Organizational Sciences, Belgrade, Serbia
milica@elab.rs

Paper introduces model for adaptive e-business continuity management (e-BCM) in insurance sector, which is adjustable to changes in the business environment of the organization. The research is focused on improvements to the establishment of effective business continuity management in insurance companies that use modern e-business technologies: the Internet, mobile computing, electronic services, virtual infrastructure, etc. The proposed model is the result of both, theoretical and practical work in the last four years. It defines a general framework for establishment and continuous improvement of e-BCM in insurance companies and includes methods for defining the key components of a business continuity management system: business impact analysis, business continuity risk assessment, and business continuity plan. The results may have broad practical application in insurance companies around the world that uses modern e-business technologies.

I. MOTIVATION

The subject of this research work is the development of a model for adaptive e-business continuity management. The research is focused on insurance companies that use modern e-business technologies (the Internet, mobile computing, electronic services, virtual infrastructure, etc.) for which reason it uses the concept of e-Business Continuity Management (e-BCM). Since e-business technologies are rapidly changing and developing, the proposed model should provide adaptive e-business continuity management, taking into account changes in the environment in which the insurance company operates. The model is developed in accordance with the ISO 22301 [1] standard, which is considered the main international standard for business continuity management and which defines the theoretical basis for establishing business continuity in an arbitrary organization.

The motive of the research is to define a general framework for the establishment and continuous improvement of e-BCM in insurance companies. In accordance with the ISO 22301 standard, the model will include methods for defining the most important components of a business continuity management system (BCMS): business impact analysis, business continuity risk assessment and business continuity plan.

II. RESEARCH QUESTIONS

The primary goal of the research is to explore possibilities of improving business continuity management in insurance sector through the development of specific model that will facilitate the establishment of e-BCM and, thanks to the adaptive component, enable successful e-BCM. Similarly to the definition of business

continuity [1], we have defined e-business continuity as the capability of an organization to continue delivery of e-services, at acceptable predefined levels of reliability and availability, following a disruptive incident.

E-business is a result of application of modern information and communication technologies (ICT): Internet technology, mobile technology, cloud computing and the next generation networks, as well as the new concepts developed on the basis of these technologies: Internet of things, big data and ubiquitous computing [2]. Apart from numerous benefits [3], modern e-business technologies create new business risks, in particular to business continuity [4][5][6] and information security, taking into account the amount, speed of creation and availability of information in modern business. The greater an organization's dependence on modern e-business technologies, the greater its vulnerability to incidents [7]. The usage of modern e-business technologies creates business and information systems that are complex in themselves and are considered to be inherently risky[5]. One of the objectives of business continuity under these circumstances becomes the ability to adapt to such emerging risks based on constant development of modern technologies, in order to protect the naturally risky systems [5].

Several different models and frameworks are described in literature that address various aspects of business continuity management, but there is a lack of a specific model that defines practical steps and procedures in establishing business continuity in insurance companies that use modern e-business technologies: the Internet, mobile computing, electronic services, virtual infrastructure, and the like.

The following common issues have been identified in existing business continuity models and frameworks: 1) Focus is placed solely on the definition and planning of the business continuity program [8] or exclusively on one aspect of business continuity management [9][10]; 2) Specific steps are missing in the definition of business continuity management [10][11][12][13][14], and, more specifically, implementation of the business impact analysis and BCM risk assessment lacks practical steps [7][15]; 3) The approach is excessively specific for a particular industry or line of business [14][16]; and 4) The approach is too complicated to be implemented in an arbitrary organization [9][10]. In addition, there is no framework specifically tailored to insurance companies.

In our work we have attempted to identify solutions to all these issues and develop a general framework that addresses all aspects of BCM and that has broad practical

application in insurance companies around the world that use modern e-business technologies.

III. METHODOLOGY

The research methodology to define model for adaptive e-BCM consists of the following general and specific scientific methods, grouped in five stages: 1) Systematized collection, review and analysis of BCM literature and existing BCM models and frameworks; 2) Initial definition of the Model for adaptive e-BCM in accordance with changes in the environment in which the organization operates; 3) Implementation of the proposed model in one insurance company; 4) Evaluation of the model by means of questionnaires and interviews with representatives of insurance company that implemented the model and 5) Final model adjustments as a result of a positive case study.

This is still work in progress, and we are currently at stage four – model evaluation stage.

IV. MODEL FOR ADAPTIVE E-BCM IN INSURANCE SECTOR

The model for adaptive e-BCM was initially theoretically defined based on ISO 22301 standard and BCM literature review. In later research stages, model has been developed and advanced from practical work. It has been successfully implemented in Insurance Stock Company “Milenijum Osiguranje” in Belgrade, Serbia which has 200 employees.

The model for adaptive e-BCM establishes, maintains and continually improves the effectiveness of insurance company’s business continuity management system (BCMS), which shields the insurance company from potential incidents (see Fig. 1).

The model consists of twelve parameters and four methods. Model parameters (see Fig. 1) reflect the basic characteristics of the business environment in which insurance company operates, from the business continuity

perspective. The model’s methods (see Fig. 2) define the key components of BCMS: 1) Business impact analysis (BIA) method; 2) e-BCM risk assessment method; 3) Method for development of business continuity plan (BCP); and 4) Method for continual BCMS improvement.

Adaptive business continuity management is essential in response to emerging risks which organizations and their information systems face due to rapid developing of e-business technologies. The model has to be adapted and applied every time there is a change in any of the model’s parameters, which enables an e-BCM that is equally flexible to both internal and external changes in the business environment of the organization. The method for continual BCMS improvement defines corrective measures for improving the BCMS. Adaptability to changes in the business environment of the organization, together with corrective measures for BCMS improvement, allows adaptive e-BCM.

A. Model Parameters

Model parameters (defined in Table 1) address the main characteristics of e-business and its underlying technologies: ubiquity, global reach, universal standards, richness, interactivity, information density, personalization/customization, and usage of social networks [17]. Parameter values are specifically tailored for insurance companies. For example, Disruption timescale (P6) is set in hours and days, as a consequence of the nature, volume, and complexity of business operations.

B. Model Methods

Each model method is precisely defined and contains a set of specific objectives and procedures. Model components – methods and associated procedures – are shown in Fig. 2, together with their related model parameters and important flow dependencies.

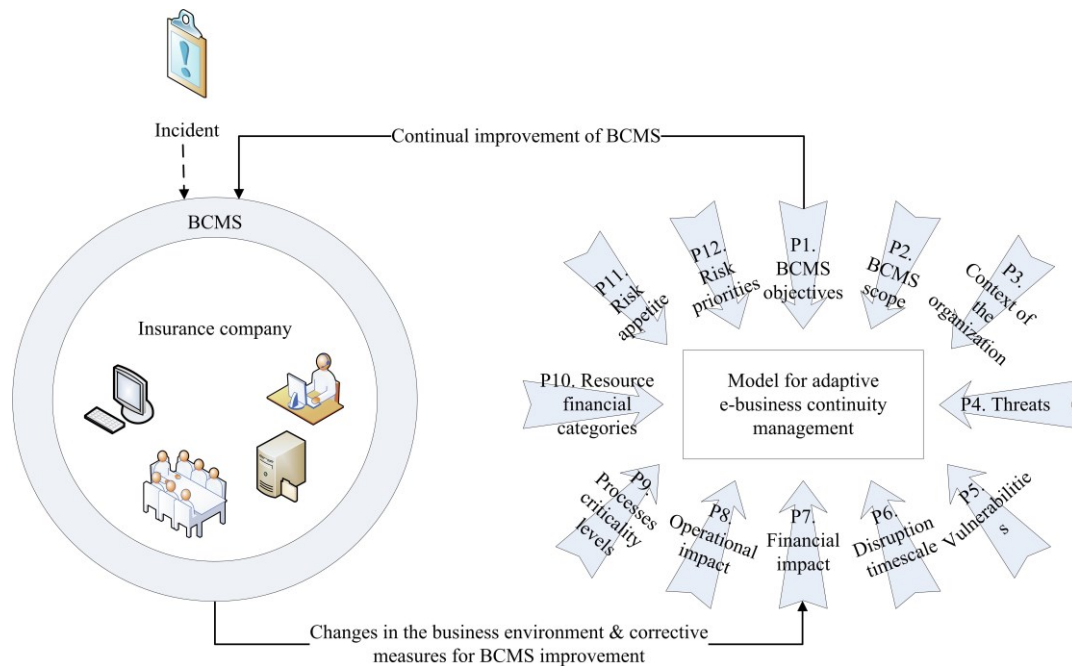


Figure 1. Model for adaptive e-BCM in Insurance Sector

TABLE I. DEFINITION OF MODEL PARAMETERS

Id.	Parameter	Description
P1	BCMS objectives	Basic objectives of BCM
P2	BCMS scope	Business processes included in the BCMS
P3	Context of the organization	Key stakeholders and legal and regulatory framework of the organization
P4	Threats	List of relevant threats to the organization
P5	Vulnerabilities	List of identified vulnerabilities of the organization
P6	Disruption timescale	Defines an adequate timescale for analyzing potential outcomes of disruption, depending on the nature of the business
P7	Financial impact	Defines whether financial impact on the business will be evaluated as part of BIA
P8	Operational impact	Defines operational impacts that are assessed as part of BIA
P9	Processes criticality levels	Defines four levels of criticality (very critical, critical, important, and vital) based on maximum acceptable outage (MAO) values
P10	Resource financial categories	Defines four resource financial categories (very high, high, medium, and low) based on financial value
P11	Risk appetite	Defines the value of acceptable level of risk for the organization
P12	Risk priority levels	Defines four risk priority levels (very high, high, medium, and low) based on risk value

1) Business impact analysis method

The purpose of business impact analysis (BIA), an integral part of a comprehensive BCMS, is to identify key business processes of the insurance company and determine how quickly these processes must recover and begin to provide complete business function after an incident. Business impact analysis identifies potential losses that may arise as the result of a disruptive incident. These losses could have an impact on business through financial, operational, regulatory, reputational, and other losses [18][19].

The objectives of BIA are: 1) Identification of key business processes and their interdependencies; 2) Identification of resources necessary for key business processes; 3) Assessment of the financial and operational impact on the insurance company in the event of a key business process outage, based on the worst case scenario; 4) Determination of recovery time objectives for key business processes: Recovery Point Objective (RPO), Recovery Time Objective (RTO) and Maximum Acceptable Outage (MAO); 5) Determination of criticality level of key business processes and prioritization of recovery activities.

The BIA method consists of procedures for: 1) Data collection and analysis at the organizational unit level; and 2) Data analysis and documentation of results at the organizational level.

2) e-BCM risk assessment method

e-BCM risk assessment should be performed for all key processes of the insurance company, not just for its IT Department [20]. Risk assessment makes an important

contribution to strategic and operational decision-making in the organization [21].

e-BCM risk assessment, as part of the BCMS, is focused on risks that can lead to interruption of business processes, while the general Risk Management Process is mostly focused on security incidents [22]. In this method we have applied an integrated approach that covers both types of incidents. This is reflected through predefined lists of potential threats and vulnerabilities for the insurance companies that are both model parameters. The potential threats and vulnerabilities in our model are focused on information systems and usage of modern e-business technologies.

The e-BCM risk assessment method consists of procedures for: 1) Risk analysis; and 2) Risk evaluation. Risk evaluation includes evaluation of critical resources of key business processes (resource value is defined as the maximum score of five assessed dimensions: confidentiality, integrity, availability, financial value, and reputational value); assessment of risk probability, i.e. likelihood of the occurrence of a threat in the presence of identified vulnerabilities, on a four-dimensional scale (Very High, High, Medium, and Low); assessment of potential impact of the risk, also on a four-dimensional scale; and determination of risk priority based on estimated risk value and risk priority levels defined as model parameters (see Fig. 2).

3) Method for development of business continuity plan

A business continuity plan (BCP) defines procedures that guide organizations to respond, recover, resume, and restore a pre-defined level of operation following a disruptive incident [1]. A BCP outlines the recovery of key business processes within recovery time objectives, as determined under the BIA method. It ensures that business processes recover rapidly and effectively, that damage to the business is minimized, and that business disruption is managed [15]. According to GCIInfotech, an IT company specializing in virtualization and cloud technologies, about 75% of organizations without an established business continuity plan will fail within three years following a major disruptive incident [23].

A business continuity plan, among other things, defines the need for different alternative locations for critical business functions, IT backups, and alternative suppliers of products/services, and considers all important issues to be observed by organizations so as to assure business continuity [24]. When defining a business continuity plan, the focus should be on data protection and preservation, since data is nowadays the most important business product [25].

A BCP can comprise one or multiple documents (sub-plans), depending on the geographical, organizational, and other business specifics of an organization. A Disaster Recovery Plan (DRP) is an important part of a BCP; the DRP defines the recovery of critical information systems and ICT resources.

The Method for development of BCP consists of procedures for: 1) Development of a BCM strategy; and 2) Development of business continuity/disaster recovery plan(s).

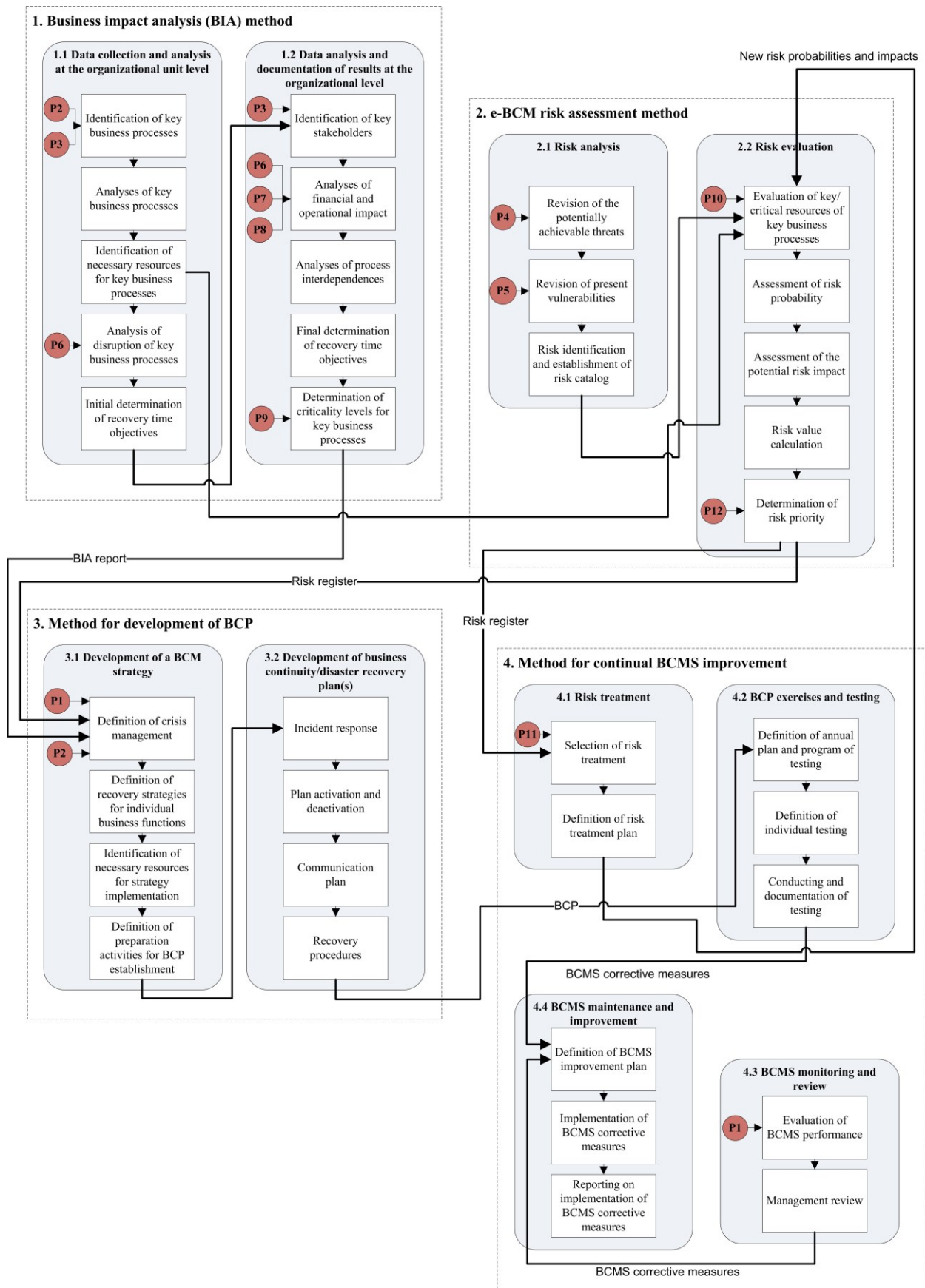


Figure 2. Model components (model parameters in circles; model methods in dotted-line rectangles; procedures, as part of methods, in rounded-corner rectangles) and important flow dependencies

4) Method for continual BCMS improvement

This method provides adaptive e-business continuity management, taking into account internal and external changes in the business environment of the insurance company and corrective measures for improvement of the BCMS. The method is applied at planned intervals and after each important change in the business environment of the organization.

The method for continual BCMS improvement consists of procedures for: 1) Risk treatment; 2) BCP exercises and testing; 3) BCMS monitoring and review; and 4) BCMS maintenance and improvement. The purpose of risk treatment is to take preventive action to address the causes and impacts of potential risk events. Except for an actual disruptive incident, BCP exercises and tests are the only way to validate BCP content and ensure that response and recovery results can be achieved within defined timeframes. BCMS monitoring and review includes evaluation of BCMS performance against BCMS objectives and management review. The goal here is to define corrective measures for BCMS improvement. It is important to conduct BCMS monitoring and review procedure at planned intervals and, in particular, after each disruptive incident that activates the BCP. The BCMS maintenance and improvement procedure implements pre-defined corrective measures designed to improve the BCMS.

V. EVALUATION RESULTS

The proposed model was successfully implemented in Insurance Stock Company “Milenijum Osiguranje” in Belgrade, Serbia which has more than 200 employees. The implementation project lasted four months, and during project 31 key business processes were identified.

To evaluate the proposed model, we established an assessment tool containing a set of evaluation criteria for main model characteristics and for each of the model methods, as defined in Table 2. For each evaluation criteria one question is formulated in the model evaluation questionnaire. All questions are assessed on a Likert five points scale, where point 1 means “strongly disagree” and point 5 means “totally agree”.

Assessment interviews were conducted with ten key users from Milenijum Osiguranje. Preliminary evaluation results support all research hypotheses, since average score of each evaluation criteria for Main model characteristics is above value of 4 (see average scores for Part 1 in Table 2). The lowest average score was for Method for continual BCMS improvement (3.4) since this method is the most advanced from the business continuity maturity perspective and its successful implementation requires some time. All other methods were averagely scored above value of 4. Our work is still in progress and we are currently in the process of performing a more exhaustive and thorough evaluation.

VI. CONCLUSION

Business continuity management is an interdisciplinary topic of broad and current interest, given the growing threat of terrorist attacks, corporate financial scandals, cybercrime, and climate change. A lack of BCM can lead to loss of revenues at best, and even to cessation of business in the worst case scenario [8]. Every organization should consider the worst possible scenario that could

TABLE II. DEFINITION OF THE MODEL EVALUATION QUESTIONNAIRE

Id.	Evaluation criteria	Av. score
Part1: Main model characteristics		4.51
Q1.1	The model defines clear and effective procedures for the establishment of e-business continuity management.	4.67
Q1.2	The model comprehensively examines the specifics of an organization's business, in particular its use of modern e-business technologies.	4.56
Q1.3	The model facilitates the establishment of business continuity in an organization that uses modern e-business technologies.	4.67
Q1.4	The model enables adaptive e-BCM in accordance with changes in the business environment of the organization.	4.44
Q1.5	The model contributes to a positive organizational attitude towards e-BCM.	4.22
Part 2: Business impact analysis method		4.50
Q2.1	The BIA is carried out as a part of the organization's key management activities.	4.44
Q2.2	The key business processes and their interdependences are identified.	4.56
Q2.3	Necessary resources of key business processes are identified.	4.33
Q2.4	Assessments of financial and operational impacts are conducted.	4.56
Q2.5	The recovery time objectives are determined.	4.67
Q2.6	The criticality levels for key business processes and recovery priorities are determined.	4.44
Part 3: e-BCM risk assessment method		4.11
Q3.1	Business continuity risk assessment process is established.	4.11
Q3.2	Results of the risk assessment are adequately documented.	4.33
Q3.3	Risk assessment is performed on regular basis.	4.22
Q3.4	Risk treatment process is established.	3.89
Q3.5	Methods of risk treatment are adequate.	4.00
Q3.6	Risk treatment plan is regularly monitored.	4.11
Part 4: Method for development of business continuity plan		4.02
Q4.1	BCMS is adequately defined.	4.44
Q4.2	Business continuity strategy is based on BIA and risk assessment results.	4.33
Q4.3	The business continuity strategy defines and provides all necessary resources in the event of a crisis situation.	4.44
Q4.4	Business continuity plan is adequately defined.	4.33
Q4.5	Business continuity plan training is adequate.	3.33
Q4.6	Business continuity plan testing is regularly performed.	3.22
Part 5: Method for continual BCMS improvement		3.4
Q5.1	BCMS performance evaluation metrics are established.	3.67
Q5.2	BCMS performance evaluations are regularly conducted.	3.56
Q5.3	Results of performance evaluation are adequately documented.	3.22
Q5.4	Adequate BCMS management review is established.	3.22
Q5.5	BCMS management review is regularly conducted.	3.22
Q5.6	BCMS management review provides decision making on the implementation of BCMS corrective measures.	3.33
Q5.7	BCMS corrective measures are adequately documented.	3.78
Q5.8	BCMS improvement plan is comprehensive and up-to-date.	3.22
Q5.9	Management is regularly informed on the status of BCMS corrective measures.	3.33

happen to their business and should determine how quickly they can recover, as well as how quickly their business can come to a point of no return. The main goal of BCM is to mitigate losses and prepare to respond effectively and efficiently in case of a major disruptive incident.

Our research is focused on improvements to establishing effective BCM in insurance companies that use modern e-business technologies. We believe that adaptive BCM is essential in response to emerging risks that insurance companies and their information systems face due to the rapid development of e-business technologies.

The proposed model for adaptive e-BCM in insurance sector is the result of our theoretical and practical work in the last four years, including implementation of the model in Insurance Stock Company "Milenijum Osiguranje". The model defines a general framework for establishment and continuous improvement of e-BCM and includes methods for defining the most important components of a business continuity management system. Final adjustments will be made to the model as a result of ongoing evaluation.

We believe that the proposed model can be applied in any insurance company that uses modern e-business technologies. We will continue this research with additional model implementations focusing on insurance and financial sectors.

ACKNOWLEDGMENT

We thank our colleagues from "Milenijum Osiguranje" who participated in the project and provided insight and expertise that greatly assisted the model implementation and our research.

REFERENCES

- [1] ISO 22301:2012 *Societal security - Business continuity management systems - Requirements*. International Organization for Standardization, 2012.
- [2] B. Radenković, M. Despotović Zrakić, Z. Bogdanović, D. Barać, and A. Labus, *Elektronsko poslovanje (eng. E-business)*. Belgrade: Faculty of Organizational Sciences, 2015.
- [3] D. Chaffey, *E-Business and E-Commerce Management - Strategy, Implementation and Practice*. 2009.
- [4] F. Arduini and V. Morabito, "Business continuity and the banking industry," *Commun. ACM*, vol. 53, no. 3, pp. 121–125, 2010.
- [5] J. Bergström, R. van Winsen, and E. Henriqson, "On the rationale of resilience in the domain of safety: A literature review," *Reliab. Eng. Syst. Saf.*, vol. 141, pp. 131–141, 2015.
- [6] M. Smith and P.-A. Shields, "Strategies for IT and communications," in *The Definitive Handbook of Business Continuity Management*, A. Hiles, Ed. John Wiley & Sons, Ltd, 2007, pp. 205–235.
- [7] J. Cook, "A Six-Stage Business Continuity and Disaster Recovery Planning Cycle.," *SAM Adv. Manag. J.*, vol. 80, no. 3, pp. 23–68, 2015.
- [8] F. Gibb and S. Buchanan, "A framework for business continuity management," *Int. J. Inf. Manage.*, vol. 26, no. 2, pp. 128–141, 2006.
- [9] S. A. Torabi, H. Rezaei Soufi, and N. Sahebjamnia, "A new framework for business impact analysis in business continuity management (with a case study)," *Saf. Sci.*, vol. 68, pp. 309–323, 2014.
- [10] K.-M. Bryson, H. Millar, A. Joseph, and A. Mobolurin, "Using formal MS/OR modeling to support disaster recovery planning," *Eur. J. Oper. Res.*, vol. 141, no. 3, pp. 679–688, 2002.
- [11] B. Herbane, D. Elliott, and E. M. Swartz, "Business Continuity Management: Time for a strategic role?," *Long Range Plann.*, vol. 37, no. 5, pp. 435–457, 2004.
- [12] R. L. Tammineedi, "Business Continuity Management: A Standards-Based Approach," *Inf. Secur. J. A Glob. Perspect.*, vol. 19, no. 1, pp. 36–50, 2010.
- [13] J. Lindström, S. Samuelsson, and A. Hägerfors, "Business continuity planning methodology," *Disaster Prev. Manag.*, vol. 19, no. 2, pp. 243–255, 2010.
- [14] H. Baba, T. Watanabe, M. Nagaishi, and H. Matsumoto, "Area Business Continuity Management, a New Opportunity for Building Economic Resilience," *Procedia Econ. Financ.*, vol. 18, no. September, pp. 296–303, 2014.
- [15] M. Savage, "Business continuity planning," *Disaster Prev. Manag.*, vol. 19, no. 5, pp. 254–261, 2002.
- [16] M. F. Blos, S. L. Hoeflich, and P. E. Miyagi, "A general supply chain continuity management framework," *Procedia Comput. Sci.*, vol. 55, no. Itqm, pp. 1160–1164, 2015.
- [17] K. C. Laudon and C. Guercio Traver, *E-commerce: business, technology, society*. 2012.
- [18] J. Watters, *Disaster Recovery, Crisis Response, and Business Continuity A Management Desk Reference*. Apress, 2013.
- [19] B. Zawada and G. Marbais, "Implementing ISO 22301," *Avalution Consulting*. 2015.
- [20] J. D. Nosworthy, "A Practical Risk Analysis Approach: Managing BCM Risk," *Comput. Secur.*, vol. 19, no. 7, pp. 596–614, 2000.
- [21] T. Aven, "Risk assessment and risk management: Review of recent advances on their foundation," *Eur. J. Oper. Res.*, vol. 253, no. 1, pp. 1–13, 2016.
- [22] S.-C. Cha, P.-W. Juo, L.-T. Liu, and W.-N. Chen, "Duplicate Work Reduction in Business Continuity and Risk Management Processes," *Res. Conf. Pap.*, vol. 9, no. Apr, pp. 25–40, 2010.
- [23] "Business Continuity is Vital to Success," *GCIInfotech*, 2014. [Online]. Available: <http://gcinfotech.com/business-continuity-is-vital-to-its-success/>.
- [24] D. Faertes, "Reliability of supply chains and business continuity management," *Procedia Comput. Sci.*, vol. 55, no. Itqm, pp. 1400–1409, 2015.
- [25] S. M. Hawkins, D. C. Yen, and D. C. Chou, "Disaster recovery planning: a strategy for data security," *Inf. Manag. Comput. Secur.*, vol. 8, no. 5, pp. 222–230, 2000.