STUDY ON INFORMATION SECURITY MANAGEMENT SYSTEM AND BUSINESS CONTINUITY MANAGEMENT IN THE CONTEXT OF THE GLOBAL CRISIS

Georg Sven Lampe[1], Mihaela Maftei[2], Ioana Surugiu[3]
and Răzvan Cristian Ionescu[4]
[1) 2) 3) 4)] The Bucharest University of Economic Studies, Romania
E-mail: georg.sven.lampe@gmail.com; E-mail: mihaela.maftei@ase.ro;
E-mail: ioana.g.surugiu@gmail.com; E-mail: razv77@gmail.com

Please cite this paper as:

Lampe, G.S., Maftei, M., Surugiu, I. and Ionescu, R.C., 2020. Study on Information Security Management System and Business Continuity Management in the Context of the Global Crisis. In: R. Pamfilie, V. Dinu, L. Tăchiciu, D. Pleșea, C. Vasiliu eds. *6th BASIQ International Conference on New Trends in Sustainable Business and Consumption.* Messina, Italy, 4-6 June 2020. Bucharest: ASE, pp. 942-949

Abstract

Parallel to the need-based expansion of business processes with new "intelligent" technologies and automated applications within digitization, the continuous further development of the technical and organizational adaptation processes to the security requirements in Business Continuity Management (BCM) from information security management system (ISMS) is indispensable. A protection against global and local threats to the value-adding business processes is required. For this purpose, the efficiency and use of measures from the ISMS must be fully integrated into the BCM, so that critical infrastructures remain unaffected in the event of disruptions outside of information security. Such value maintenance is central to the relationship between business continuity, business strategy and information security. However, the strategic potential for managing global risks in emergency and crisis situations, such as epidemics and pandemics through crisis management (CM) within the BCM of ISMS, is largely unexplored. Many service companies show different approaches to business continuity and how to deal with specific threats. Therefore, the previous model of information processing and business continuity for emergency and crisis situations must be brought into line and with expanded measures. Practical principles for the analysis and implementation of risk management process (RMP) as well as key factors are presented, which draw attention to an improved preservation of value. Technical, organizational and personnel processes that ultimately connect the quantitative measures to be assessed and the bodies involved must be described with a quality of action that is classified by the ISMS according to quality and risk parameters for the BCM.

Keywords

Business continuity management, crisis management, risk management, information security management, digitization, risk processes, pandemic

JEL Classification

L15, L98, M10, M15, Q43, Q48

Introduction

The studies carried out by the authors propose to investigate the extension of the existing Risk Management Process (RMP) within the Business Continuity Management (BCM) and its impact on the measures of crisis management (CM) due to the epidemic / pandemic risk threat on the information security of the critical infrastructure managed supply and telecommunication services. According to ISO 22301 (2019), the RMP approaches for BCM are comparable and primarily relate to disruptions that can occur due to globalization and internationalization with outsourcing, out tasking and the involvement of numerous business partners. Local and global aspects such as epidemics / pandemics are specified here. Health aspects such as epidemics / pandemics are not specified in ISO 27001 (2013) in conjunction with the BCM. Therefore, the BCM from the ISMS must be supplemented by the epidemic / pandemic category with the corresponding measures. BCM has proven to be a systematic process to reduce the effects of crises and disruptions due to increasing threats in many industries. For this, preventive business continuity strategies and operational emergency and crisis plans are derived. It provides a framework for the own resilience of the business processes against risks and offers the possibility to protect the added value, the interests of the stakeholders and the reputation (Gibb and Buchanan, 2006). The companies should take the current emergency and crisis as an opportunity to adapt the existing emergency and crisis planning by the crisis management and if necessary to optimize it (Herbane, 2010). Furthermore, the prioritization of business processes according to the Business Impact Analysis (BIA) enables a restart in the correct order. Professional crisis communication allows companies to control social media as well as internal and external stakeholder groups instead of being controlled by them.

Literature Review

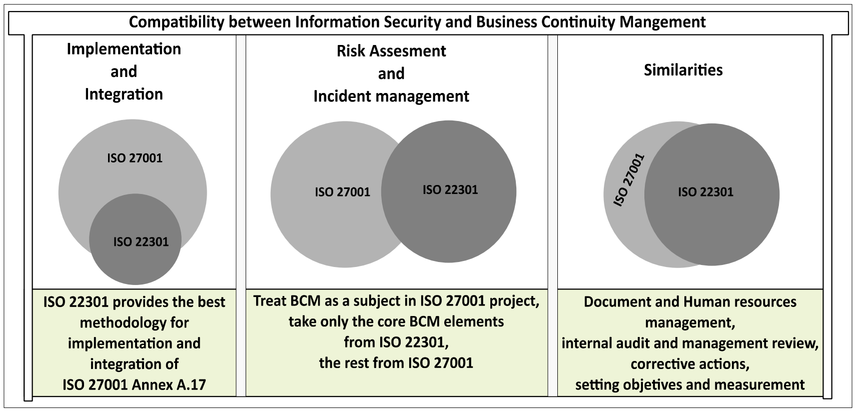
Organizations should adopt the principle of business continuity having a solid base that provides the opportunity of synchronizing the business continuity management with the existing management systems (Maier et al., 2014). Business continuity management systems (BCMS), information security management systems (ISMS), risks management systems (RMS), emergencies and crises management systems (CMS) today mainly depend on information and communication technology (ICT) based services and the associated risks. The increasing digital networking simplifies joint communication, coordination and cooperation (3C) and increases the competitiveness of companies. But at the same time, security threats (e.g. cyber-attacks) are increasing due to digital change. However, legal concerns and requirements for data security and protection are perceived as obstacles in digital transformation (Marquardt et al., 2018). An innovative digital transformation of systems and processes in companies also puts their ability to absorb resources to the test, as many show signs of overload (Cho et al., 2016; Järveläinen, 2012). All aspects that are necessary for the continuation of the critical business processes in the case of a damage event must be considered and not only information or telecommunications technology resource (Herbane et al., 1997). Availability and capacity processes are also important in order to provide information about the status and location of the human and IT resources that are critical in case of disruption (Ionescu et al., 2019). The IT emergency and crisis management of BCM within the ISO 27001:(2013) is consequently that shall ensure information security is therefore part of the BCM emergency management from ISO 22301. A holistic approach of the RMP for global and complex risks is therefore crucial in order to be able to react quickly and effectively to emergency situations (World Economic Forum, 2020). Due to the currently critical impact of a longer downtime of ICT services caused by the threat to public health in the event of an epidemic / pandemic, the importance of ICT-based fully automated supply of energy and telecommunications is emphasized (Lampe and Massner, 2018).

Research Methodology

Two methods are used to achieve the research goals. The first part of this work focuses on the theoretical aspects and the current state of knowledge of research articles, laws, international standards, best practices and studies on the management systems for business continuity, information security, risks, emergencies and crises. The second part represents the "practical" and "empirical" section of this study. For this study, business impact analysis (BIA) and the RMP methodology were carried out within critical infrastructures to complying information security. This is on the one hand due to the fact that operators of critical infrastructures within the meaning of the IT Security Act are committed to certify, after the BSI critical ordinance has been passed. On the other hand, the BCM only considers the availability of information in accordance with ISO 22301 and how the operational processes are guaranteed in the event of a crisis. Protection objectives such as confidentiality, integrity, availability and authenticity of information's are not considered in this standard. For this intent, quantitative descriptive approaches were used to identify organizational variables (risks and controls) for the protection objectives, which can explain the success or failure of technical and organizational implementation efforts. The international standards on ISMS describe how operational continuity management should be implemented. Therefore, the existing model of information processing is to be expanded to include the elements for implementation. As a result, the second part examines the organizational requirements and the measures to be used by the BCM within the ISMS. A conceptual approach is being developed to demonstrate that the BCM also has a role for critical infrastructures in crisis situations within the ISMS. Within the analysis of the organizational measures used, supplemented by a specific literature search, authors intended to investigate whether the expansion of the BCM from the ISMS by integrating an epidemic / pandemic plan, the level of maturity and other information security management processes such as risk and communication could be improved.

Research Results and Discussion

The analysis of the specific literature showed that for the operators of business processes within the energy and telecommunications services as well as for operators of critical infrastructures, specific standards and guidelines that define the requirements for the ISMS and the BCM were issued. According to ISO 27001, the ISMS is intended to ensure effective protection of information and IT systems with regard to confidentiality, integrity and availability. For these risks, the legislative in Germany has set a "reasonable security" against threats to the grid control binding (§11 paragraphs 1a and 1b of the Energy Industry Act 2005 and the IT Security Act 2015). The IT Security Catalogs (SICAT) of the German Federal Network Agency specifies the security requirements for an "adequate security". Network management related recommendations have to be complied in future as well. The key point of these requirements can be summarized in proof (as of 2018) of a functioning and certified ISMS according to ISO 27001 in combination with ISO 27002 (2013) and ISO 27019 (2017). According to BSI-Kritis Regulation (2016), energy network operators or energy grid operators of critical infrastructures were also legally obliged to report IT security incidents towards the German Federal Office for Information Security. This means that the core requirements for compliance with the protection objectives were set by the legal framework for energy network operators and energy system operators. In addition, the ISMS includes a BCM and is required to be implemented by the IT security law. The BCM from the ISMS begins with an analysis of the business impact and a threat analysis that identifies events, which can lead to an interruption of business operations and business processes. Once the threat is identified and registered through incident handling, a risk assessment must be performed to determine the business impact, likelihood of occurrence, and recovery time required for critical business applications and processes. This assessment takes into account only those business processes that relate to information technology. This includes, for example, preventive and reactive measures in the cyber room against viruses. However, the international standards on ISMS don't describe how BCM should be implemented, as shown in Figure no. 1.


Compatibility between Information Security and Business Continuity Mangement
Implementation and Integration
ISO 27001
ISO 22301
Risk Assesment and Incident management
ISO 27001
ISO 22301
Similarities
ISO 27001
ISO 22301

ISO 22301 provides the best methodology for implementation and integration of ISO 27001 Annex A.17

Treat BCM as a subject in ISO 27001 project, take only the core BCM elements from ISO 22301, the rest from ISO 27001

Document and Human resources management, internal audit and management review, corrective actions, setting objetives and measurement

Fig. no. 1 Similarities and overlapping areas of ISO 27001 and ISO 22301
Source: Authors, 2020.

The ISO 22301 should be used for this intent, in order to reduce the risks of any kind of business interruption and to take the best possible precautions in the event of serious disruptions. Possible serious disruptions can be:

- Natural disasters such as floods or earthquakes;
- blackouts and fires;
- Disruptions and damage to the infrastructure;
- social and political upheavals such as unrest and political upheavals;
- local and global health issues such as epidemics or pandemics;
- Personnel or material losses due to attacks or accidents.

The main reasons for this are, on the one hand, increasingly IT-supported operating processes, and on the other hand, globalization and internationalization with outsourcing, out tasking and the integration of numerous business partners around the world. An intensive analysis of ISO 22301 shows that the view of risk management in particular is somewhat more special and is characterized by the terms as business impact analysis, business continuity strategies, solutions and risk assessment. The BIA is concerned with identifying potential problems and to evaluates them. The part of the BCM-RMP is mainly concerned with planning and testing potentially failing assets that would cause significant damage to the organization if they failed. The BCMS-RMP generally only plans or tests the failure of individual assets or subsystems in the organization. The basis for this is the BIA, emergency concepts and regular exercises (training). With regard to the protection objectives, only the availability of information and the operational processes in the event of a disaster are considered within ISO 22301, but not the protection objectives such as confidentiality, integrity and authenticity of information. Achieving the availability of data, which from the point of view of the information systems is the main objective of business continuity, is therefore also one of the main objectives of ISM. An organization's information security architecture is influenced by information security policies, risk management, internal and external audits. The objective of information security policy must be ensured so that employees understand the importance of information security and business continuity and act accordingly. Risk management is required to identify and assess information security assets and threats. It is therefore recommended to extend data security (authenticity) and data protection (intervenability, non-connectivity and transparency) within ISO 27001 with integrated BCM by the associated protection objectives. However, the accumulation of the mutual linking of risks threaten entire societies, economies and international relationships. In order to answer the question of what risks exist for the assets of a company (assets) within the framework of the ISMS and BCM, regulations and protection objectives are defined. In addition, criteria for the acceptance of residual risks are specified. Based on the maximum development of product and service deliveries within energy and telecommunications, the following approach to risk assessment with regard to business activity is recommended:

- ISO 27001 for BSI 100-4 (2009) and IT Security Act catalogue - §11 paragraphs 1a and 1b of the Energy Industry Act as the basis for the power generation and distribution;
- Risk management adaptation for information security – compatibility with ISO 27002;
- IT security techniques – Information security risk management ISO 27005 (2018);
- Business Continuity Management ISO 22301;
- Determination of the potential conflict regarding the independent influence due to market situations for the provision of products and services;
- Determination of the confidentiality of substitute values for missing measured values as a function of time (expected value from measured value modelling);
- Risk reduction through a system regulation approved by the energy supplier.

Risk management is an iterative process of listing, evaluation and handling using the methods of international standards. This risk reduction should be done under the condition ALARP "as low as reasonably practicable", i.e. the reduction to a level which allows the highest practical level of security with financially and technically justifiable effort. For this, the defined measures of the catalogue of controls are to be processed in their order and the risk treatment to mitigate threats is set. Selected controls are offered in several stages according to the defence-in-depth principle – increasing security and continuity by setting up several parallel security mechanisms – and are classified as follows:

- preventative: Physical access security, authentication and authorization, filters/firewall, training and awareness;
- revealing: Surveillance cameras, logging and monitoring, security and compliance scanning, firewall, security audits and reviews;
- correcting: Protection of operating procedures, intrusion prevention, security patching, incident response, emergency response.

The degree of achieving the fulfilled controls leads to a result, which in case of over-fulfilment represents a chance and a problem in case of under-fulfilment. Detected issues require re-capture, analysis, assessment, and policy definition. Detected problems require reanalysis, assessment and policy definition. With risk management approaches standard, conventional risks can be relatively easily isolated and humanity understands very well how to mitigate these risks. Fundamental elements such as energy and resource efficiency, renewable energies and sustainability are increasingly on the agenda of today's companies. Energy policies should be focused on sustainability and concerned in safeguarding a clean and healthy environment, as well as energy efficiency. Due to the compatibility of ISO 27001 and ISO 22301, the business processes to be assessed must be expanded with reasonable effort for the BCM with regard to the occurrence of serious disruptions in the ISMS threat catalogue. The organizational adaptation of roles and responsibilities is primarily to be carried out by the newly established emergency and crisis team. Proactive action measures in the event of a crisis enable employees to act in a targeted and structured manner in an emergency. Careless decisions and actions, especially in time-critical situations and under enormous emotional stress, can have significant negative effects without a defined crisis management process. Professional crisis communication allows companies to control the press, social media and internal and external stakeholder groups instead of being controlled by them. If additional knowledge from the training and, if applicable, real events are used for the targeted updating, adaptation and further development of BCM, the BCM has reached its highest level of maturity. In the event of a pandemic, it must be possible to take the first measures within a few hours to days in order to have a minimal impact on staff availability. This is only possible by planning the preventive and reactive measures beforehand. Preventive measures are mainly aimed at preventing infection and the spread of the virus. Above all, this includes awareness-raising measures and the implementation of specific measures to prevent (initial) infection. A great deal of importance must be attached to awareness-raising measures, in particular, because the development of new viruses cannot guarantee the effectiveness of measures implemented to date. As a result, only the employee can prevent infection. A sensitized employee is more able to make an informed decision and thus reduce the risk of infection. This also applies to information security, which is significantly influenced by the actions of people in an organization. If an infection has already occurred, the reactive measure, the quarantine and the use of alternative resources to maintain an emergency operation are appropriate. In information technology, it is even advisable to go one step further and use preventive means to separate systems with different protection requirements using segmentation of IT networks. The pandemic plan becomes part of the BCM within the ISMS and represents the framework for effective pandemic management. This should consist of concrete and clear instructions, such as compile checklists for the implementation review. The four levels of the pandemic plan and business continuity planning by 3C within information security are presented below in figure no. 2.

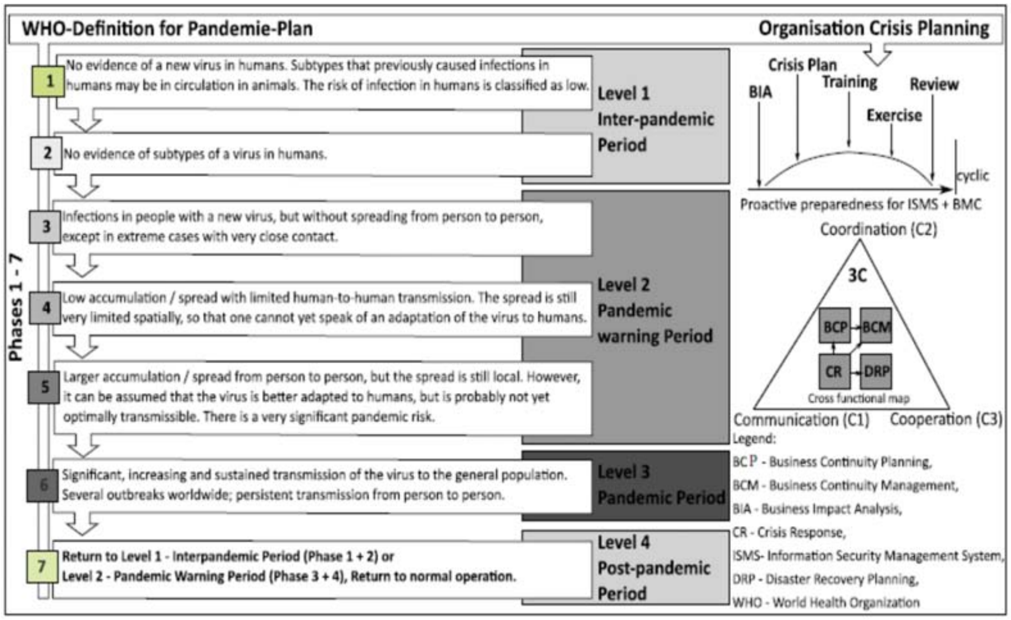

WHO-Definition for Pandemie-Plan
Organisation Crisis Planning
Phases 1 - 7
1
No evidence of a new virus in humans. Subtypes that previously caused infections in humans may be in circulation in animals. The risk of infection in humans is classified as low.
2
No evidence of subtypes of a virus in humans.
Level 1 Inter-pandemic Period
3
Infections in people with a new virus, but without spreading from person to person, except in extreme cases with very close contact.
4
Low accumulation / spread with limited human-to-human transmission. The spread is still very limited spatially, so that one cannot yet speak of an adaptation of the virus to humans.
5
Larger accumulation / spread from person to person, but the spread is still local. However, it can be assumed that the virus is better adapted to humans, but is probably not yet optimally transmissible. There is a very significant pandemic risk.
Level 2 Pandemic warning Period
6
Significant, increasing and sustained transmission of the virus to the general population. Several outbreaks worldwide; persistent transmission from person to person.
Level 3 Pandemic Period
7
Return to Level 1 - Interpandemic Period (Phase 1 + 2) or Level 2 - Pandemic Warning Period (Phase 3 + 4), Return to normal operation.
Level 4 Post-pandemic Period
Crisis Plan
BIA
Training
Review
Exercise
cyclic
Proactive preparedness for ISMS + BMC
Coordination (C2)
3C
BCP
BCM
CR
DRP
Cross functional map
Communication (C1)
Cooperation (C3)
Legend:
BCP - Business Continuity Planning,
BCM - Business Continuity Management,
BIA - Business Impact Analysis,
CR - Crisis Response,
ISMS- Information Security Management System,
DRP - Disaster Recovery Planning,
WHO - World Health Organization

Fig. no. 2 Pandemic plan related to business continuity into ISMS

Source: Authors, 2020.

The BCM within the ISMS must include controls to identify and mitigate global risks, limit the consequences of harmful incidents, and ensure that business operations or processes are restarted in good time. BCM is often seen as part of information security because breaches of information security are one of the many possible threats to business continuity. The business continuity in the processes and structures is ensured through regular reviews and updates of the business continuity plans. Internal and external audits are used within the organization to receive feedback on the organizational and technical measures of the business processes from the ISM and BCM.

Conclusions

With the ISMS, many protection objectives can be achieved and the information integrity within an organization can be guaranteed. In addition, business continuity can be well represented in a general management framework along with the associated additions of controls and control objectives. Although daily management activities derived from the Plan-Do-Check-Act are assigned to the management framework, in order to go beyond compliance and aim towards information security excellence, more advanced tools, as Six Sigma and EFQM, that foster innovation and digital transformation are needed (Olaru et al., 2017; Hohan et al., 2015). The additions take into account specific topics such as policy, organization, personnel, inventory, IT operations and IT communication as well as business continuity management from the ISMS perspective. While the BCM system of ISO 22301 always focuses on the "potential crisis", ISO 27001 looks at everyday business life. Although ISO 27001 provides a good basis for the development of an ISO 22301-compliant system, its implementation usually means a systematic approach throughout the organization. If ISO 22301 is implemented alone, this can only be done for selected parts and not in completely. If an ISO 27001- compliant system already exists, it can build on its results. This expansion creates added value for the organization, since essential management procedures have been tried and tested. All that is required here is to add "BCM-specific points", which results in an integrated management system. The security threats from cyber-attacks in intelligent automation and digitization structures and the probability of serious disruptions such as epidemics / pandemics are increase. By continuously developing the management of information security and information security risks during digital changes and the occurrence of global serious influences, disruptions in business process and business continuity management can be minimized.

References

Bundesamt für Sicherheit in der Informationstechnik (BSI), 2016. *BSI-Kritis Regulation (Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz: BSI-KritisV)*, [online] Available at: <https://www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html> [Accessed at 17 April 2020].

Cho, C.S., Chung, W.H. and Kuo, S.Y., 2016. Cyberphysical Security and Dependability Analysis of Digital Control Systems in Nuclear Power Plants. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 46(3), pp.356–369.

Federal Office for Information Security, 2009. *BSI Standard 100-4: Business Continuity Management*, [online] Available at: <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-4_e_pdf.pdf?__blob=publicationFile&v=1> [Accessed at 17 February 2020].

German Federal Network Agency, 2015. *IT security requirements catalog in accordance with Section 11 (1a) of the Energy Industry Act (IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz)*.

Gibb, F. and Buchanan, S., 2006. A framework for business continuity management. *International Journal of Information Management*, 26(2), pp.128–141.

Herbane, B., 2010. The evolution of business continuity management: A historical review of practices and drivers. *Business History*, 52(6), pp.978–1002.

Herbane, B., Elliott, D. and Swartz, E., 1997. Contingency and continua: achieving excellence through business continuity planning. *Business Horizons*, 40(6), pp.19–25.

Hohan, A.I., Olaru, M. and Pirnea, I.C., 2015. Assessment and Continuous Improvement of Information Security Based on TQM and Business Excellence Principles. *Procedia Economics and Finance*, 32(2015), pp.352–359.

International Organization for Standardization, 2013a. *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements*. Geneva: ISO.

International Organization for Standardization, 2013b. *ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls*. Geneva: ISO.

International Organization for Standardization, 2017. *ISO/IEC 27019:2017 Information technology — Security techniques — Information security controls for the energy utility industry*. Geneva: ISO.

International Organization for Standardization, 2018. *ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management*. Geneva: ISO.

International Organization for Standardization, 2019. *ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements*. Geneva: ISO.

Ionescu, R.C., Olaru, M. and Sargut, K., 2019. Study of the Information Security Impact on the Business Continuity. In: K. Soliman, ed. *Proceedings of the 34th International Business Information Management Association Conference (IBIMA)*. Norristown, Pa: IBIMA, pp.4279–4287.

Järveläinen, J., 2012. Information security and business continuity management in interorganizational IT relationships. *Information Management & Computer Security*, 20(5), pp.332–349.

Lampe, G.S. and Massner, S., 2018. Informationssicherheit in Energienetzen. In: I.G. im V. (ITG), ed., *Mobilkommunikation : Technologien und Anwendungen : Vorträge der 23. ITG-Fachtagung, 16.-17. Mai 2018 in Osnabrück*. Berlin: VDE Verlag, pp.115–121.

Maier, D., Olaru, M., Floricel, T. and Marin, G., 2014. Innovative Integrated Management Systems for the Business Continuity Management. In: V. Grozdanic, ed. *Proceedings of the 10th European Conference on Management Leadership and Governance (ECMLJ 2014)*, Proceedings of the Conference on European Management Leadership and Governance. Reading: Acad Conferences LTD, pp.482–486.

Marquardt, K., Olaru, M., Golowko, N. and Kiehne, J., 2018. Study on Economic Trends , Drivers and Developments of the 21 St Century. In: R. Pamfilie, V. Dinu, L. Tachiciu, D. Plesea and C. Vasiliu, eds. *BASIQ The 4th international Conference on New Trends in Sustainable Business and Consumption*. Heidelberg: ASE, pp.65–73.

Olaru, M., Ionescu, R.C., Maftei, M. and Ilie, C., 2017. Application of Six Sigma tools for improvement of Information Security Management System. In: K. Soliman, ed. *Proceedings of the 30th International Business Information Management Association Conference, IBIMA 2017 - Vision 2020: Sustainable Economic development, Innovation Management, and Global Growth*. Norristown, Pa: IBIMA, pp.5779–5784.

World Economic Forum, 2020. *The Global Risks Report 2018*. 15th ed. [pdf] *The Global Risks Report 2020*, Geneva: World Economic Forum. Available at: <http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf> [Accessed 17 Apr. 2020].