Transdisciplinary Engineering for Complex Socio-technical Systems – Real-life Applications
J. Pokojski et al. (Eds.)

doi:10.3233/ATDE200125

Components of the Preliminary Conceptual Model for Process Capability in LGPD (Brazilian Data Protection Regulation) Context

Gianfranco MUNCINELLI[a,1] , and Edson Pinheiro DE LIMA[a.b], Fernando DESCHAMPS[a], Sergio E. Gouvea DA COSTA [a,b], José Marcelo A. P. CESTARI[c]
[a] *Industrial and Systems Engineering Graduate Program, Pontifical Catholic University of Parana – Curitiba, Brazil*
[b] *Federal University of Technology - Parana – Curitiba, Brazil*
[c] *Federal University of Parana – Curitiba, Brazil*

Abstract. A capability model describes the complete set of features that an organization requires to execute its business model or fulfill its mission; the user's environment must be increasingly included in the design and development of necessary and desired solutions. For this, the development of the model and its application are central issues. An account should be taken of legislation involving the protection of individuals' personal data in any relationship involving the processing of information classified as personal data; as well as its impact on public and private companies across the country, considering any size and market segment, and taking into account the need to comply with legal requirements efficiently and sustainably, mitigating risk factors. Transdisciplinarity characterizes this research, as the digital transformation process integrates legal, technological aspects, risks, business analysis, good practices and standards of information technology management and digital compliance. This paper addresses this problem by analyzing the main areas of contribution to the assessment of process capability for digital transformation concerning cybersecurity in the context of personal data protection legislation. Finally, the main components of the future capability model are presented.

Keywords. Process Capability, LGPD, transdisciplinary engineering.

Introduction

A capacity model describes the complete set of resources an organization requires to execute its business model or fulfill its mission. For this, the development of the model and its application are central issues. This means that data needs to be actively managed at all stages of the data life cycle (that is, collected, stored, analyzed, shared, and archived) through defined data practices, standards and policies. Law 13.709 / 2018 impacts private and public companies across the country, considering any size and market segment, taking into account the need to meet requirements efficiently and

[1] Corresponding Author, Mail: gmunci@hotmail.com / g.muncinelli@pucpr.edu.br.

sustainably. Legislation (LGPD – Lei Geral de Proteção de Dados - General Data Protection Law) involving the protection of individuals' personal data in any relationship that involves the processing of information classified as personal data. The business process must take into account the need to meet legal requirements efficiently and sustainably, mitigating risk factors.

This work is part of the doctoral thesis of one of the authors and is a direct result of the systematic literature review. It is an initial study that forms the basis of the doctoral thesis, therefore, with still partial results. Information security is not only a matter of Information and Communication Technology organizations, but also of increasingly interconnected industrial and service environments; they are no longer isolated corporate systems and must be protected. Systems of service companies are especially vulnerable to attacks and threats such as people's mistakes, incidents on employees' devices, cyberattacks, disgruntled workers, external access, cloud computing, and data leaks. Transdisciplinarity characterizes this research, as the digital transformation process integrates legal, technological aspects, risks, business analysis, good practices and standards of information technology management and digital compliance.

The legislation is new, and the work intends to help society and companies to think about the adequacy strategy since there is no single product or action that guarantees the suitability of a company to the LGPD. It is understood that there must be a clear strategy, which includes legal, technological, and management process aspects.

This article addresses this problem by analyzing the main areas of contribution to assessing the capacity of the digital transformation process concerning cybersecurity in the context of personal data protection legislation. The main objective is to present the main components of the future capability model to understand the functionality and the underlying flows in the LGPD context.

1. Research Design

An initial (preliminary) analysis of the literature related to the processing capacity and the process improvement models published in the leading magazines from 2000 to 2019 is made. The initial step is to define the set of guidelines that served as a starting point for this work, based mainly on several leading structures such as COBIT, ITIL, and ISO27001. Two different aspects must be part of the model: 1) risk management, regarding regulatory aspects; 2) the cost-benefit ratio, related to the company's business process and financial results.

The research in this work was carried out in two phases. In the first phase, a search was carried out with the keywords derived from the initial readings, in works published in journals and conferences. An additional clarification: "CAPES Portal" is a virtual library that brings together and makes available to teaching and research institutions in Brazil the best of international scientific production. In the second phase, some of the main references in the field were analyzed to identify areas of contribution for future research and characterization of the current research. The procedures for each of the phases will be explained during this document. Results of the first phase were obtained by modifying a procedure for the analysis of co-citation of authors, found in the literature [1]. The modified procedure was composed of the steps shown in figure 1, below:

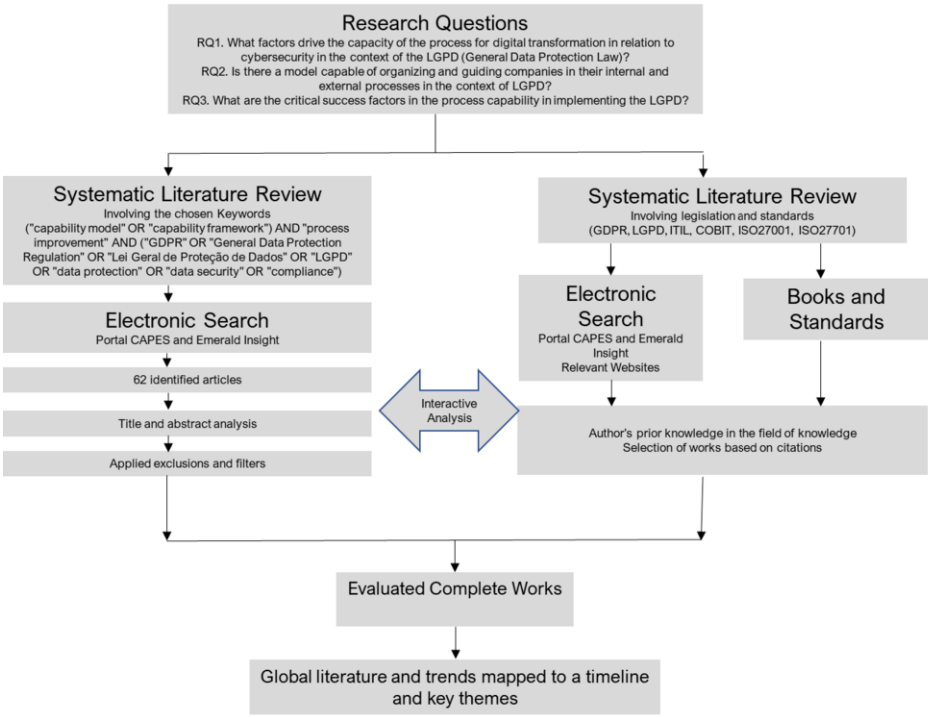

Figure 1. Research Design.

In the second phase, three research axes are established: 1) Capability Model; 2) Processes improvement; 3) Data Protection. After a few searches, the final set of search words, shown in figure 2, was defined.

The reference databases were searched for jobs related to the field informally and loosely. There are two main objectives with this approach. The first objective is to determine whether a keyword generates relevant results. The second objective is to determine whether a specific reference database contains relevant works that include the keyword. The result of the loose screening step is a set of reference databases and a set of keywords to be searched.

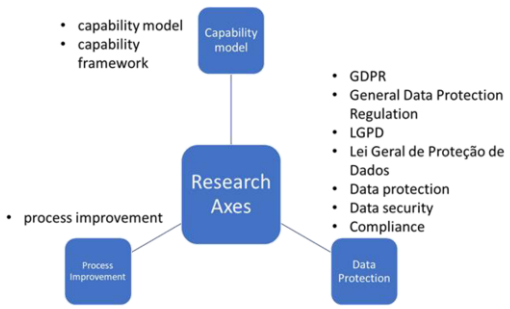

Figure 2. Definitive keywords.

The criteria for selection in the databases were: publication date from 2010 to 2019; Journal articles and English language - as shown in Table 1, for the search engine Portal Capes and Emerald Insight.

Table 1. Literature Review Protocol - Portal Capes and Emerald Insight search engine.

Search words	("capability model" OR "capability framework") AND "process improvement" AND ("GDPR" OR "General Data Protection Regulation" OR "Lei Geral de Proteção de Dados" OR "LGPD" OR "data protection" OR "data security" OR "compliance")	
Boolean Operator	AND, OR	
Database	Portal CAPES, selecting Science Direct Journals (Elsevier), Emerald Insight, Elsevier (CrossRef), Scopus (Elsevier)	Emerald Insight
Language	English	English
Publication Type	Paper from journals	Paper from journals
Period	2010 until 2019 (03/09/2019)	2010 until 2019 (03/09/2019)
Result	40 articles	16 articles

The next step was to download all 56 articles found, to obtain information such as authors, journal or conference, year, keywords, references, and abstract. The interest is also to obtain the full text of the article for further analysis. The records were organized and analyzed to filter duplicate papers and to identify papers that were not related to the subject of our study. This was done by analyzing the title, abstract, and keywords and, when necessary, the full text. The list of works with their records was later exported to an electronic spreadsheet in which they could be treated and analyzed. Twenty-six articles were removed because they are not related to the research theme.

2. Literature Analysis

About future developments that could be derived from the analysis carried out in this work, there are two main areas of contribution to be observed: (i) construction of the model that allows decision making for companies immersed in this context of LGPD and; (ii) the implementation of the model.

Regarding the construction of the model, the main concepts are coming from the following articles: Zou [2] addresses the mapping of the processes for collecting, analyzing, and approving safety information and the communication system. The integration of the ideas of reference structures, capacity maturity models, and improvement processes in the construction of a holistic metamodel [3]. Other industries and applications have not adopted electronic readiness models. However, CMMs, although initiated in software engineering, has progressed to incorporate construction models that encompass processes as diverse as management and financial documentation. Suggests that a CMM is more applicable to applications such as e-commerce in construction [4]. The validation of the cybersecurity structure of socio-technical systems requires time and continuous monitoring in a real-life environment [5]. Support the continued growth of IT-enabled health service models; Compliance with new regulation [6]. Service quality; quality assessment structure is the focus of the study from Domınguez-Mayo [7]. Steuperaert shows the framework for information and technology governance and management [8]. Lack of a common or shared understanding of compliance management concepts is a barrier to effective compliance management

practice [9]. The risk concerning the regulatory agency is another subject to be added to the study [10]. The digitalization potential of your business processes [11]. The establishment of clear reference points to allow each agency to determine a roadmap for a greater maturity of electronic contracting [12]. The digital transformation requires the integration of specialized information and communication technology resources [13]. Decision support for IT service managers who want to improve service management processes [14]. The context of multi-regulations with a complex and interconnected information system [15]. The importance of context awareness [16]. Process-oriented developments [17]. Size and sector in the proposed multidimensional model of process capability dimensions [18]. The application of socio-technical systems theory to the domain of information and cybersecurity, where much emphasis is placed on security software and hardware resources [5], To better understand the innovation relationship of IT capacity service from the perspective organizational mechanisms (organizational agility, organizational learning, and entrepreneurial alertness) [19]. Business process management (BPM) is considered the principle of best practice management that can help companies maintain a competitive advantage [20]. Risk management in several selected ISO standards to provide the basis for improving, coordinating, and interoperating risk management activities in IT configurations for various purposes related to quality management, project management, IT service management, and information security management [21]. The construction of process metamodels; the cost of non-quality; budget; Balanced Scorecard perspective; requirements x processes; reactive x proactive models [22].

Concerning the implementation of the model aspects found: Main concepts are that the failure in the implementation occurs due to the maturity of the companies not being taken into account during the definition phase [23]. Classification of relevant issues in the assessment and development of the case for the adoption of the model during the definition phase [24]. Those organizations can choose to structure process improvement projects using various implementations to facilitate the transfer of knowledge within and between units [25]. The motivations, resistances, facilitators, and results of the collaboration [26]. Operational guide for industries to evaluate their distribution processes based on the concept of capacity/maturity [27]. Compliance with new regulation [28]. The introduction of new quality standards can provide the framework for the development and formulation of new innovative business models - the positive view of implementing new regulation [29], and the restrictions or recommendations for the management and performance measurement systems [30][31].

After this analysis, seven main concepts are obtained (A - Business process management; B - Continuous monitoring; C - Standards and best practices; D - New Regulation Compliance; E - Continuous quality assessment framework; F - Risk Analysis; G - Business and context analysis.), which can be grouped in table 2.

Table 2. Seven main concepts.

Author	A	B	C	D	E	F	G
Abdullah (2016)	X						
Balint (2016)	X	X					X
Baraforta (2017)	X					X	
Benmoussa (2015)	X		X				X
Buglione (2013)	X	X			X	X	X
Carroll (2016)			X		X		X
Concha (2012)	X		X				
Cuzzocrea (2019)	X						X
Denner (2018)	X						X
Díaz-Ley (2010)	X	X	X		X		X

Domınguez-Mayo (2015)	X				X		
Eadie (2012)			X	X	X		
Fawcett (2012)	X	X				X	X
Gonzalez-Rojas (2016)				X	X		
Harun (2012)	X		X				
Malatji (2019)					X		
Malatji (2019)	X				X		X
Mayer (2019)				X	X		X
Mc Caffery (2010)				X		X	
McHugh (2012)				X			
Nadarajah (2014)	X		X		X		
Ongena (2019)	X						X
Reyes (2010)	X						
Shrestha (2016)	X				X		
Smart (2010)	X	X			X		X
Steuperaert (2019)			X	X			
Tsou (2018)			X				
Van Looy (2018)							X
Van Looy (2019)	X						
Zou (2017)	X	X					X

3. Additional Literature

The acronym COBIT stands for Objectives Control for Information and Related Technology. It is the most recognized and used knowledge base in the market to support organizations in Information Technology Governance (IT) [32].
COBIT 5 is based on 5 principles that create a kind of direction for the system of governance and management of information and related technology used within an organization [32]. The 5 COBIT principles are: Principle 01 - Meet the needs of stakeholders; Principle 02 - Cover the organization from end to end; Principle 03 - Apply a single and integrated framework (model); Principle 04 - Allow a holistic approach; Principle 05 - Distinguish governance from management.

ITIL is an acronym for Information Technology Infrastructure Library; it is a set of detailed best practices for IT service management that focuses on aligning IT services with business needs [33]. ITIL describes processes, procedures, tasks, and checklists that are neither organization-specific nor technology-specific but can be applied by an organization to establish integration with the organization's strategy, delivering value and maintaining a minimum level of competence. It allows the organization to establish a baseline from which to plan, implement, and measure. It is used to demonstrate compliance and measure improvement. There is no independent third party compliance assessment available for ITIL compliance in an organization [33].

ISO standards are based on the concept of Management System, that is, how activities are coordinated to direct and control an organization with its objectives. That is how activities are organized, carried out, and supervised to achieve a specific objective (ISO).

ISO / IEC 27001: 2013 [ISO / IEC 27001: 2013] Information technology - Security techniques - Information security management systems. It specifies the requirements to establish, implement, maintain, and continuously improve an information security management system in the context of the organization. It also includes requirements for the assessment and treatment of information security risks, adapted to the needs of the organization. The requirements established in ISO / IEC 27001: 2013 are generic and must apply to all organizations, regardless of type, size, or nature [34].

ISO / IEC 27701: 2019 [ISO / IEC 27701: 2019] - Security techniques - Extension to ISO / IEC 27001 and ISO / IEC 27002 for privacy information management - Requirements and guidelines. This document specifies requirements and guides establishing, implementing, maintaining, and continuously improving a Privacy Information Management System (PIMS) in the form of an extension of ISO / IEC 27001 and ISO / IEC 27002 for managing privacy in the context of the organization. Besides, it specifies the requirements related to PIMS and guides personally identifiable information controllers (PII) and PII processors responsible and responsible for PII processing. This document applies to all types and sizes of organizations, including public and private companies, government entities, and non-profit organizations, which are PII controllers and PII processors that process PII within an ISMS (Information Management System) Information Security) [35].

4. Components of the Preliminary Conceptual Model

Any changes to the company's structure or service processes would have a direct or indirect impact on customers and stakeholders (including regulatory authorities). However, it depends on what those changes are. The response to the regulatory context may be a risk or an opportunity since the National Data Protection Agency (ANPD) has not yet regulated some aspects of the law. There are two main areas of contribution to be observed: building the model that allows decision making for companies immersed in the LGPD context and; (ii) the implementation of the model.

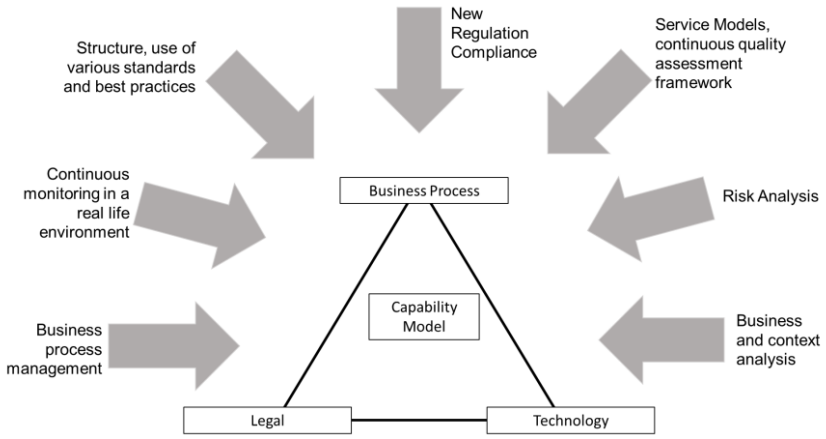

Figure 3. Main components of the model.

Thus, derived from the analysis the main components of the model and preliminary that we see are (shown in figure 3): 1) Business process management; 2) Continuous monitoring in a real-life environment; 3) Structure, use of various standards and best practices; 4) New Regulation Compliance; 5) Service Models, continuous quality assessment framework; 6) Risk Analysis; 7) Business and context analysis.

Capability is the ability to perform a repetitive pattern of actions that is necessary to create value for the customer.

A business capability is a fundamental element of what a company does or can do. It is an abstraction of the functionality and the underlying flows expressed as a substantive form. An agglomeration of a cluster of underlying business resources can manifest a product, service, platform, business unit, department, and, of course, a company.

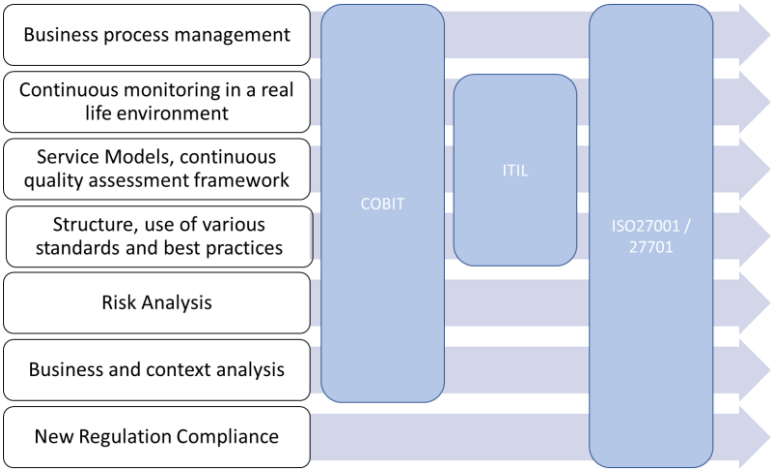

Figure 4. Main components of the model related to the additional literature.

Figure 4 shows the main components of the model related to the additional literature. A capability model (or business capabilities map or capabilities model) is a structurally sound and internally logical group of capabilities; this main components will be the base for the following steps that are being constructed at the doctorate thesis of the author (figure 5).

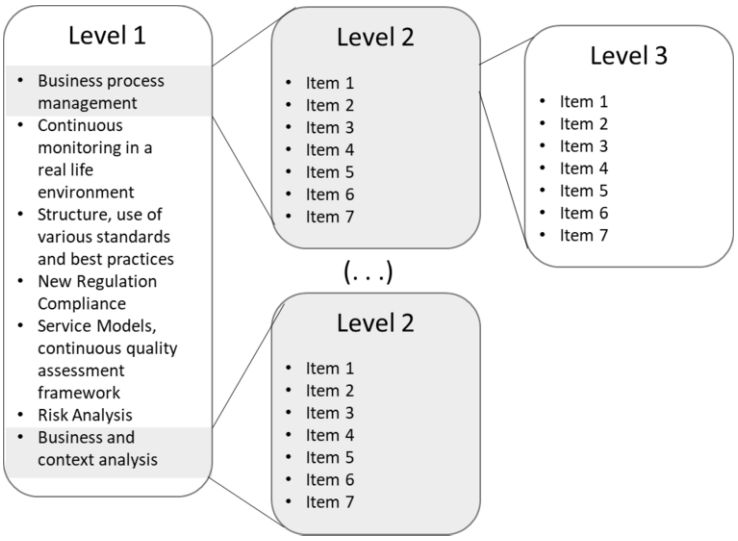

Figure 5. Generic structure of the future capability model.

5. Conclusions

The main objective of this work was to present the main components of the future capability model to understand the functionality and the underlying flows in the LGPD context. Research lines were found to go in different directions, being aligned with the research problem explicitly related to the General Data Protection Law (LGPD), which provides us with a field of action to be explored. In any case, existing research supports the construction and implementation of decision-making models. Thus, the main components of the future capability model we see are: 1) Business process management; 2) Continuous monitoring in a real life environment; 3) Structure, use of various standards and best practices; 4) New Regulation Compliance; 5) Service Models, continuous quality assessment framework; 6) Risk Analysis; 7) Business and context analysis.

Taking into account the complementary concepts of the good practices already used today, the model will evolve with the concepts of COBIT, ITIL, and ISO27001 / 27701. COBIT brings the direction for the system of governance and management of information and related technology used within an organization. ITIL has focused on aligning IT services with business needs. ISO shows the concept of Management System - how activities are coordinated to direct and control an organization concerning its objectives.

References

[1] S. Eom, Author co-citation analysis: quantitative methods for mapping the intellectual structure of an academic discipline, *Information Science Reference*, 2009, vol. 49, no. 13, p. 347.
[2] P.X.W. Zou, P. Lun, D. Cipolla, S. Mohamed, Cloud-based safety information and communication system in infrastructure construction, *Safety Science*, 2017, Vol. 98, pp. 50–69.
[3] H.G. Reyes, R. Giachetti, Using experts to develop a supply chain maturity model in Mexico. *Supply Chain Management: An International Journal*, 15/6 (2010) 415–424
[4] R. Eadie, S. Perera, G. Heaney, Capturing maturity of ICT applications in construction processes. *Journal of Financial Management of Property and Construction*, Vol. 17, No. 2, 2012 pp. 176-194.
[5] Malatji, Masike; Von Solms, Sune; Marnewick, Annlizé. Socio-technical systems cybersecurity framework, *Information & Computer Security*, Vol. 27 No. 2, 2019 pp. 233-272.
[6] N. Carroll, I. Richardson, Software-as-a-Medical Device: demystifying Connected Health regulations, *Journal of Systems and Information Technology*, Vol. 18, No. 2, 2016 pp. 186-215.
[7] F.J. Domınguez-Mayo, J.A. Garcıa-Garcıa, M.J. Escalona, M. Mejıas, M. Urbieta, G. Rossi, A framework and tool to manage Cloud Computing service quality. *Software Qual J* (2015) 23:595–625.
[8] D. Steuperaert, COBIT 2019: A SIGNIFICANT UPDATE. *The EDP Audit, Control, and Security Newsletter*. 2019. 59:1, 14-18
[9] N.S. Abdullah,; M. Indulska, S. Sadiq, Compliance management ontology – a shared conceptualization for research and practice in compliance management. *Inf Syst Front* , 2016, 18:995–1020.
[10] F. McCaffery, J. Burton, I. Richardson, Risk management capability model for the development of medical device software, *Software Qual J*, 2010, 18:81–107.
[11] M.-S. Denner, L.C. Püschel, M. Röglinger, How to Exploit the Digitalization Potential of Business Processes, *Bus Inf Syst Eng*, 2018, 60(4):331–349.
[12] G. Concha, H. Astudillo, M. Porrúa, C. Pimenta, E-Government procurement observatory, maturity model and early measurements, *Government Information Quarterly*, 29 (2012) S43–S50
[13] O. Gonzalez-Rojas, D. Correal, M. Camargo, ICT capabilities for supporting collaborative work on business processes within the digital content industry, *Computers in Industry*, 80 (2016) 16–29.
[14] A. Shrestha, A. Cater-Steel, M. Toleman, Innovative decision support for IT service management, *Journal of Decision Systems*, 2016, 25:sup1, 486-499,
[15] N. Mayer, J. Aubert, E. Grandry, C. Feltus, E. Goettelmann, R. Wieringa, An integrated conceptual model for information system security risk management supported by enterprise architecture management. *Software & Systems Modeling*, 2019, 18:2285–2312.

[16] A. Van Looy, J. Van den Bergh, The Effect of Organization Size and Sector on Adopting Business Process Management, *Bus Inf Syst Eng*, 2018, 60(6):479–491.
[17] A. Van Looy, J. Devos, A roadmap for (un)successful BPM: positivist case studies, *Business Process Management Journal*, 2019, Vol. 25, No. 5, pp. 1164-1190.
[18] G. Ongena, P. Ravesteyn, Business process management maturity and performance - A multi group analysis of sectors and organization sizes, *Business Process Management Journal*, 2019, pp. 1463-7154.
[19] H.-T. Tsou; C.C.J. Cheng, How to enhance IT B2B service innovation? An integrated view of organizational mechanisms, *Journal of Business & Industrial Marketing*, 2018, 33/7, pp. 984–1000.
[20] D. Nadarajah, S.L. Kadir, A. Syed, A review of the importance of business process management in achieving sustainable competitive advantage, *The TQM Journal*, 2014, Vol. 26, No. 5, pp. 522-531.
[21] B. Baraforta, A.-L. Mesquidab, A. Mas, Integrating risk management in IT settings from ISO standards and management systems perspectives, *Computer Standards & Interfaces*, 2017, 54, pp. 176–185.
[22] L. Buglione, C.G. von Wangenheimc, F. McCafferyd, J.C.R. Hauck, The LEGO strategy: Guidelines for a profitable deployment, *Computer Standards & Interfaces*, 2013, 36, pp. 10–20.
[23] M. Díaz-Ley, F. García, M. Piattini, MIS-PyME software measurement capability maturity model – Supporting the definition of software measurement programs and capability determination, *Advances in Engineering Software*, 2010, 41, pp. 1223–1237.
[24] A. Smart, Exploring the business case for e-procurement, *International Journal of Physical Distribution & Logistics Management*, 2010, Vol. 40, No. 3, pp. 181-201.
[25] B. Balint,; C. Forman, S. Slaughter, Effectiveness of knowledge transfer mechanisms for implementing process improvement frameworks in services offshoring. Journal of Management Information and Decision Sciences, 2016, Vol. 19, No. 1.
[26] S.E. Fawcett, A.M. Fawcett, B.J. Watson, G.M. Magnan, Peeking inside the black box: toward an understanding of supply chain collaboration dynamics, *Journal of Supply Chain Management*, Vol. 48, Number 1. 2012, pp. 44-72.
[27] R. Benmoussa, C. Abdelkabir, A. Abd, M. Hassou, Capability/maturity based model for logistics processes assessment - Application to distribution processes, *International Journal of Productivity and Performance Management*, 2015, Vol. 64, No. 1, pp. 28-51.
[28] M. McHugh, F. McCaffery, V. Casey, Software process improvement to assist medical device software development organisations to comply with the amendments to the medical device directive. *IET Softw.*, 2012, Vol. 6, Iss. 5, pp. 431–437.
[29] K. Harun, K. Cheng, An integrated modeling method for assessment of quality systems applied to aerospace manufacturing supply chains, *Journal of Intelligent Manufacturing*, 2012, 23:1365–1378.
[30] A. Cuzzocrea, F. Folino, M. Guarascio, L. Pontieri, Predictive monitoring of temporally-aggregated performance indicators of business processes against low-level streaming events, *Information Systems*, 81, 2019, pp. 236–266.
[31] E. Pinheiro de Lima,; S.E. Gouvea da Costa, J.J. Angelis, The strategic management of operations system performance, *International Journal of Business Performance Management*, 2008, 10(1): 108-132.
[32] G. Blokdyk, *Cobit A Complete Guide*. 5STARCooks, 2018.
[33] AXELOS. *ITIL Foundation: ITIL 4 Edition*. Axelos, 2019.
[34] ISO/IEC 27001:2013 Information security management systems. 2013.
[35] ISO/IEC 27701:2019 Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. 2019.