

Maturity Models for Business Continuity—A Systematic Literature Review

Diogo Pinto^{1*}, André Fernandes¹, Miguel Mira da Silva¹, Rúben Pereira²

¹ Instituto Superior Técnico, INOV - Instituto de Engenharia de Sistemas e Computadores Inovação, Universidade de Lisboa, Av. Rovisco Pais 1, 1049-001 Lisboa, Portugal

² Instituto Universitário de Lisboa (ISCTE-IUL), Cidade Universitária de Lisboa, Av. das Forças Armadas, 1649-026 Lisboa, Portugal

Corresponding Author Email: andre.fernandes@inov.pt



<https://doi.org/10.18280/ijss.120115>

ABSTRACT

Received: 10 October 2021

Accepted: 12 January 2022

Keywords:

business continuity, process reference model, process assessment model, maturity model

Business continuity refers to the planning and preparation done ahead of time to ensure that an organization's essential business processes can continue to work in the event of an emergency. Natural disasters, business crises, pandemics, workplace crime, or any other incident that disrupts business operations are examples of emergencies. Maturity models provide companies with a way to assess their relative implementation for a management framework. This paper provides a Process Assessment Model for Business Continuity based on a Systematic Literature Review. The selected articles from the literature provide information about the state-of-the-art in this research field, an understanding of the numerous research activities that have been undertaken in recent years, and a forecast of potential developments.

1. INTRODUCTION

Business Continuity is a management process that aims to identify the potential threats that will lead to a business disruption of an organization [1]. The process of managing Business Continuity became more complex over time due to the increased complexity of the information systems and the constant rise of new threats to the organizations, and this has led to the Business Continuity Management to mainly focus on the processes that are critical to the organization [2]. A business continuity framework can help strengthen the organization's resilience, providing an effective response to the previously identified disruptions [1].

Business Continuity Plans are developed to scope the organization's critical processes and mainly cover the priorities for the organization's recovery after a major disaster occurs [1]. To aid the organizations in the implementation and evaluation of the Business Continuity several standards can be followed, some of those being a Process Reference Model and a Process Assessment Model.

The Process Reference Model includes processes that can already exist in a scope of a management system. These processes will be the basis of the Process Assessment Model, the Process Assessment Model allows the performance of assessments on organizations reporting the results using a scale of capability and processes. The results of the assessment performed can be used to improve the performance or identify risks associated with the processes [3].

One or more Process Assessment Models must be the basis for a Maturity Model. Maturity Models can translate how an organization can grow to higher levels of a specific process [3].

The Process Reference Model aids the organizations by clearly defining the processes of a given scope. Due to the complexity of the area of Business Continuity, a Process Reference Model and a Process Assessment Model would help

the organizations to become more efficient in the management of Business Continuity.

To the best of our knowledge, there are no Process Assessment Models or any Process Reference Models in the scope of Business Continuity developed and presented by the ISOs. Research in the literature was performed to verify what was developed by other authors. Our goal is to develop a Process Reference Model and a Process Assessment Model for Business Continuity to fill the lack of those in the ISOs, specifically the lack for the ISO22301 [4].

To create the Process Reference Model and the Process Assessment Model, the authors decided to rely on the literature to get the information needed. The methodology used was the Systematic Literature Review (SLR) [5]. This methodology allowed the authors to verify state of the art by answering the Research Questions mentioned in section 3.1 while identifying the Processes and extracting them alongside their Inputs, Outputs, and Outcomes.

After identifying and extracting the Processes, Inputs, Outputs, and Outcomes, this data was analyzed. By the end of the peer-reviewing process, the authors created a Process Assessment Model based on the information gathered and analyzed in the literature. The methodology used to create the Process Assessment Model will be later explained in the paper in section 3.3, Reporting Phase.

2. THEORETICAL BACKGROUND

2.1 Business continuity

Business Continuity is the organization's ability to continue delivering products or services at acceptable predefined levels following a disruptive incident [6], business continuity allows to checking how the organization was affected by a disaster,

what was the impact, and how they can recover from the losses caused by the disruption of service [7].

There are several approaches to put in practice the Business Continuity Plans, one of them is divided into a four-stage cycle [1]:

- The first step of this cycle is the Mitigation Phase, where the risks are identified, managed, and reduced;
- The second step is the Readiness Phase, all the measures identified for the critical processes are implemented;
- The third step is the Response, when a crisis occurs, the organization must be able to manage all the emergencies;
- In the Recovery Phase, after a crisis occurs, the organization must identify what needs to be done for the business to return as usual.

A Business Continuity Plan is developed to avoid or mitigate risks, reduce the impact of a catastrophe and reduce the time needed for the organization to return to business as usual. The Business Continuity Plan should be dynamic, evolving as the business environment changes and adapt to these changes [8].

2.2 ISO 22301

ISO 22301 is a standard for business continuity management that “specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise” [6]. This standard specifies requirements for setting up and managing an effective Business Continuity Management System.

A Business Continuity Management System emphasizes four main topics [9]: The importance of understanding the organization’s needs and the necessity for establishing business continuity management policy and objectives. The implementation and operational controls and measures for managing an organization’s overall capability to manage disruptive incidents. Monitoring and reviewing the performance and effectiveness of the Business Continuity Management System. A continual improvement based on objective measurement. The requirements specified are generic and intended to be implemented in all organizations, regardless of their size, field of work, the country where they operate, and its type.

To keep the Business Continuity Plan updated this standard follows the Plan-Do-Check-Act model which is divided into four phases. The first phase, the Plan phase, establishes the business continuity policy, objectives, targets, controls, processes, and procedures relevant to improving business continuity. The second phase, the Do phase, implements and operates the business continuity policy, controls, processes, and procedures. The third phase, the Check Phase, monitors and reviews performance against business continuity policy and objectives. By last, the Act phase maintains and improves the Business Continuity Management System by taking corrective actions based on the results of management review [6].

2.3 Process reference model, process assessment model and maturity model

A process as defined in ISO 33001 is a “set of interrelated

or interacting activities which transforms inputs into outputs”. The process elements include: process purpose statements, process outcomes, and process performance indicators. According to ISO 33052, "A process reference model is a model comprising definitions of processes described in terms of process purpose and outcomes, together with an architecture describing the relationships between the processes. Using the Process Reference Model in a practical application may require additional elements suited to the environment and circumstances" [10].

ISO 33004 specifies the requirements for a Process Reference Model, a Process Assessment Model, and a Maturity Model. It also states how these Models must be evaluated and what competencies the testers must ensure.

According to the ISO 33004, the purpose of the Process Reference Model is to “define a set of processes that collectively can support the primary aims of a community of interests, provides the basis for one or more process assessment models” [3].

There are Requirements that the Process Reference Models must obey:

- The domain of the Process Reference Model must be declared.
- The connection between the Process Reference Model and the intended context of use must be provided.
- A description of the processes that are connected within the Process Reference Model must be provided.

The community of interests and the actions that must be performed to achieve them are documented in the Process Reference Model.

When performing an assessment, a Process Assessment Model is the practical implementation of one or more Process Reference Models. The main difference between a Process Assessment Model and a Process Reference Model is the fact that the Process Assessment Model has Inputs, Outputs, and Outcomes related to the same processes as the Process Reference Model. This additional information makes the Process Assessment Model available for the performance of an assessment [3].

We can get the Maturity Model from a set of one or more Process Assessment Model. The level of maturity of a process can be calculated through the assessment of a Process Assessment Model [11] where the Maturity Model can be represented by a scale of organizational process maturity that identifies at which level a process of a Process Assessment Model is and specifies what the requirements that need to be achieved for a process to reach higher levels are.

The main difference between a Process Assessment Model and a Maturity Model is that the Process Assessment Model analyses the capability of the processes by ranking them on a scale of capability dimension and processes, while the Maturity Models take into account the process maturity [11].

To verify if the Process Reference Model, Process Assessment Model, and Maturity Model are well implemented in the assessment is verified if the requirements are met either by demonstrating conformity or demonstration of compliance.

3. RESEARCH METHODOLOGY

In this paper, the authors analyzed the Process Reference Model, Process Assessment Model [10], and the Maturity Models [3] to understand in detail how they were developed and how much information was present in these standards.

A Systematic Literature Review is a methodology that provides a systematic and rigorous method to review and analyze the literature. A Systematic Literature Review aims to aggregate all existing evidence on a research question and support the development of evidence-based guidelines for practitioners [5].

A Systematic Literature Review is divided into the following phases:

- Planning - we explain our motivation along with the objectives that we aim to achieve, expressed using Research Questions.
- Conducting - we create a search string and use that string in multiple databases to find papers related to the search query topics.
- Reporting – we analyze the results by answering the Research Questions.

3.1 Planning phase

Our motivation to perform this review comes from the fact that there are not any Process Reference Models nor any Process Assessment Models in the scope of Business Continuity in the ISOs. To research more about this topic, the authors analyzed the literature to search for Process Reference Models and Process Assessment Model developed outside the ISOs. Without the existence of the Process Reference Models and the Process Assessment Models, our goal is the

development of those with the aid of the Systematic Literature Review Methodology.

The authors performed the Systematic Literature Review to understand and analyze the state of the art of literature in this domain and gather information for developing the Process Reference Model and the Process Assessment Model. To develop the Maturity Models, the authors extracted the Processes, Inputs, Outputs, and Outcomes that will be used to answer the Research Questions.

To achieve these objectives, the authors formulated one main Research Question (RQ1) composed of three others (RQ1.2, RQ1.3, RQ1.4). The sub-questions were developed in order to provide more consistency and clearness to this research because, as mentioned in section 2.3, according to ISO 33001, the main elements in the structure of a process are its inputs, outputs and outcomes:

- RQ1: What are the Processes of Business Continuity Management?
 - a. RQ1.2: What Inputs exist?
 - b. RQ1.3: What Outputs exist?
 - c. RQ1.4: What Outcomes exist?

The Search String that we used to answer the questions is presented in Table 1. The first column was searched in the title, the second column in each paper's abstract, and the conjunction 'OR' joined them together. If a paper had these two criteria met, it would be included in our list of chosen papers.

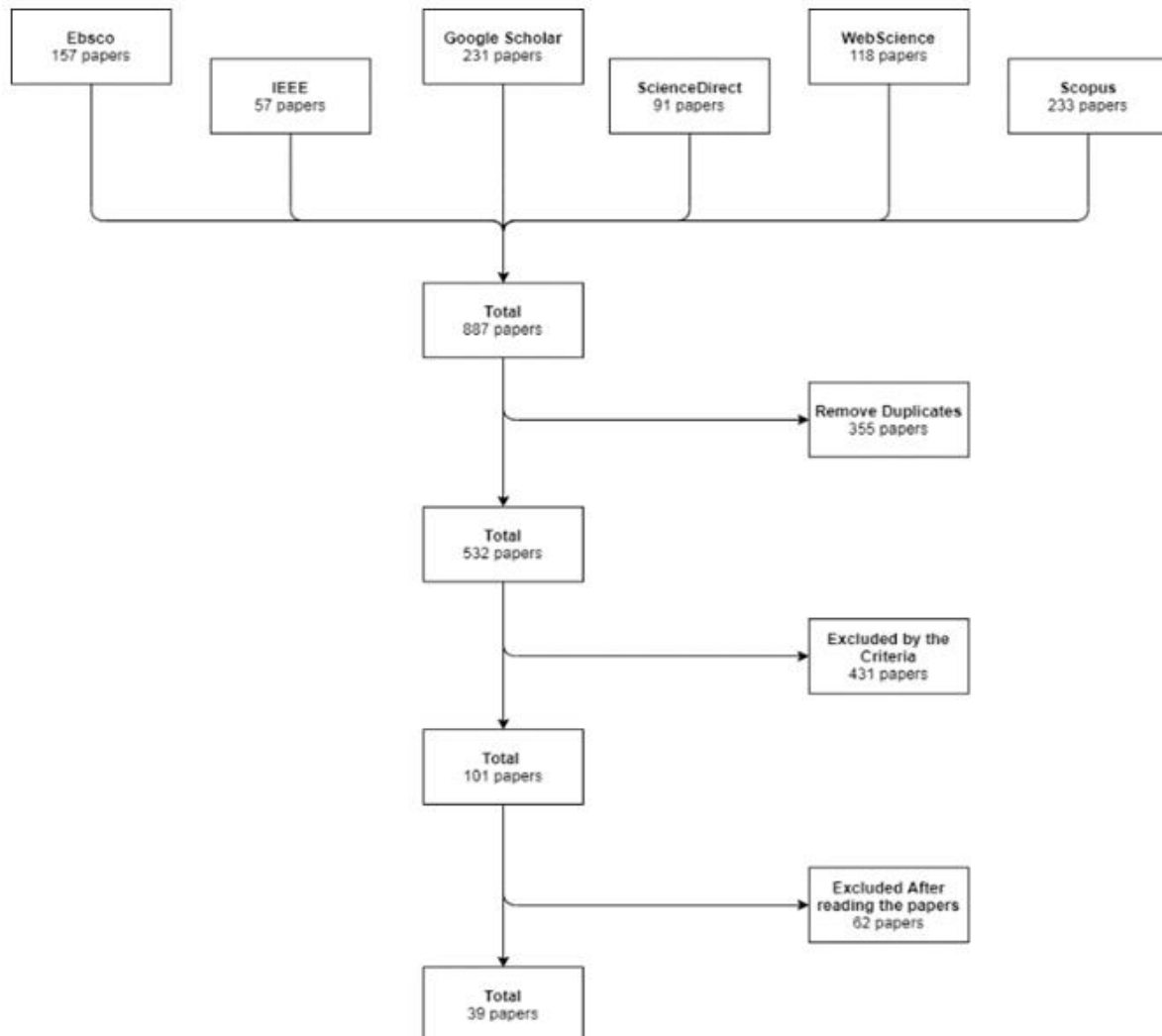


Figure 1. Methodology of the systematic literature review

Table 1. Search string used for the review

Title	Abstract
'Maturity Models' OR	'Business Continuity' OR
'Maturity Model' OR	'Disaster Recovery' OR
'standards' OR	'Business Continuities' OR
'standard'	'Disaster Recoveries' OR
	'Disasters Recoveries' OR
	'Process' OR
	'Method' OR
	'Framework' OR
	'Methodology' OR
	'Activity'

The databases were the following: ScienceDirect, IEEE Digital Library, Scopus, Google Scholar, Ebsco, and Web of Science.

The inclusion and exclusion criteria must be applied to filter the obtained papers. The inclusion criteria were the following: the scope was Maturity Models for Business Continuity, and Peer-Review. The exclusion criteria were: Articles of Opinion, Articles Out of Scope, Not Written in English, and Maturity Models of other domains.

3.2 Conducting phase

After applying the search string in the databases selected, we found 887 articles. After removing the 355 duplicates, we read the abstract and applied the inclusion and exclusion criteria. At the end of this process, 101 articles remained. These 101 papers were read, and after excluding the articles according to the previously defined criteria, we ended up with 39 papers. This method is summarized in Figure 1. The papers selected are presented in Table 2.

Table 2. Literature business continuity processes

Reference	Title
[12]	Business Continuity Management in a Dynamic Environmental Lessons from Macondo
[13]	A Methodology for Developing a Business Continuity Strategy
[14]	Talking about a (business continuity) revolution: Why best practices are wrong and possible solutions for getting them right
[15]	Implementing business continuity management systems and sharing best practices at a European bank
[16]	Information Management Procedures for Business Continuity Plan Maintenance
[17]	Area business continuity management, a new approach to sustainable local economy
[18]	Area business continuity management, a new opportunity for building economic resilience
[19]	Business continuity management: a systemic framework for implementation
[20]	The effect of business continuity management factors on organizational performance: A conceptual framework
[21]	Assessing business continuity requirements
[22]	Application impact analysis: A risk-based approach to business continuity and disaster recovery
[23]	Reliability of supply chains and business continuity management
[24]	Business Continuity Plan: Examining of Multi-Usable Framework
[25]	A framework for business continuity management
[26]	Business continuity management planning methodology
[27]	Business continuity management: time for a strategic role?
[9]	A Literature Review on Business Continuity Based on ISO 22301, Six Sigma and Customer Satisfaction Evaluation
[28]	Issues in business continuity management
[29]	COBIT 5 domain delivery, service and support mapping for business continuity plan
[30]	Information technologies for business continuity: an implementation framework
[31]	Business continuity plan design
[32]	COBIT-ITIL mapping for business process continuity management
[33]	Adaptive e-business continuity management: Evidence from the financial sector
[34]	Business continuity planning methodology
[35, 36]	Interdisciplinary review of business continuity from an information systems perspective: toward an integrative framework
[37]	Implementation of the IT governance standards through business continuity management: Cases from Croatia and Bosnia-Herzegovina
[38]	Fujitsu's Business Continuity Plan Development Methodology
[39]	How prepared are small and medium sized companies for Business Continuity Management?
[7]	Business continuity management guidelines
[40]	Business continuity plan using ISO 22301:2012 in IT solution company
[2]	A business continuity management maturity model for the UAE banking sector
[41]	A model driven engineering approach for business continuity Management in e-Health systems.
[42]	A Normative Process Model for ICT Business Continuity Plan for Disaster Management in Small, Medium and Large Enterprises.
[1]	Business Continuity
[43]	Creating meaningful business continuity management programme metrics
[44]	Business continuity management for supply chains facing catastrophic events
[45]	System view of business continuity management
[35]	Business continuity management: A standards-based approach
[46]	A model-driven framework for process-centric business continuity management

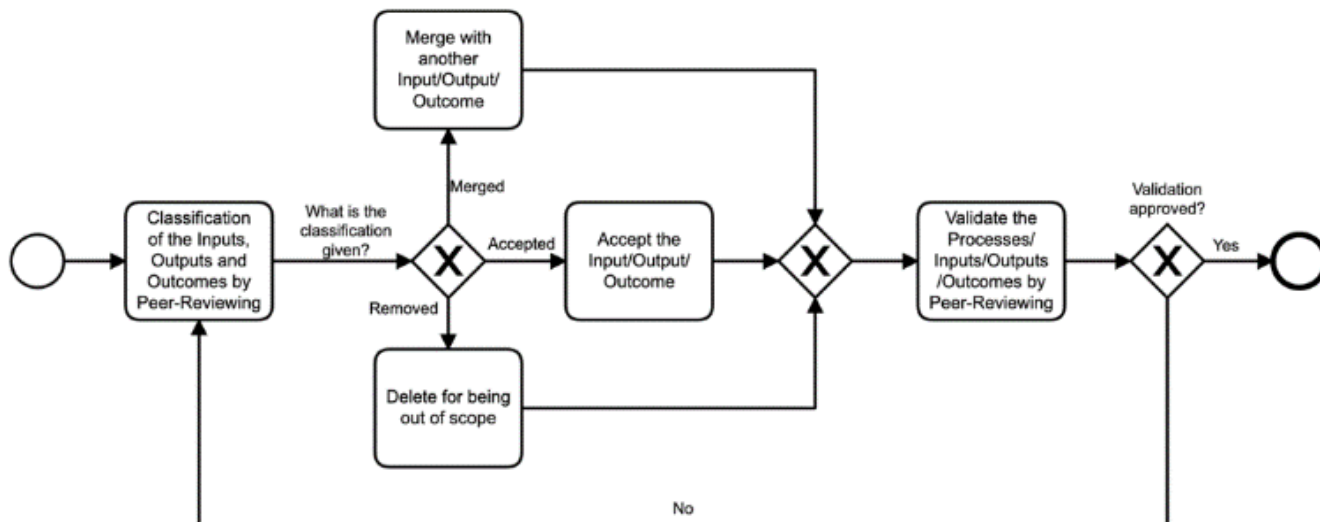


Figure 2. Validation of an input, output and outcome

Table 3. Final processes after consolidating the processes found

Processes	Definition	Papers
Planning Management	Planning ensures the organization's operations are secure and functional when even the worst-case scenario becomes a reality.	31
Risk Management	Risk Management ensures the identification of risks and disruptions to the organization's prioritized activities, systematically analyze risk, evaluate which disruption related risks have required treatment and, identifies treatments commensurate with business continuity objectives	29
Requirements Management	Requirements Management ensures the analysis of business continuity requirements based on the data that supports the action plan development.	10
Prevention Management	Prevention Management ensures the identification of an organization's exposure to internal and external threats and synthesizes hard and soft assets to provide effective prevention and recovery.	6
Implementation Management	Implementation Management ensures to put in place any improvements to operating procedures, infrastructure, security, etc., which can help to transfer, minimize or absorb the risks of processes and services being compromised	4
Monitoring	Monitoring ensures to determine what needs to be measured, the methods for monitoring, when the monitoring and measuring shall be performed and when the results shall be analyzed and evaluated.	4
Mitigation Management	Mitigation Management ensures the testing of the risk mitigation strategies and the disaster recovery plans are carried out both regularly and comprehensively to see whether the plans are still relevant and deliverable.	4
Exercise and Testing	Exercise, Testing and Monitoring ensures that the business continuity procedures are consistent with its business continuity objectives	3
Policy Management	Policy Management ensures that a business continuity policy is established that is appropriate to the purpose of the organization, provides a framework for setting business continuity objectives, includes a commitment to satisfy applicable requirements	3
Impact and Recovery Management	Impact Management ensures the protection of the prioritized activities, mitigates, responds and manages impacts	3
Strategy Support	Strategy Support ensures that the organization determines and provides the resources needed for the establishment, implementation, maintenance and continual improvement of the Business Continuity Management Strategy.	2

3.3 Reporting phase

The last phase of the Systematic Literature Review is the Reporting Phase, in which we answer the Research Questions.

To gather all the Inputs, Outputs, and Outcomes, the authors extracted from each paper the Processes and all the information regarding those Processes (the Inputs, Outputs, and Outcomes). After this step, the acceptance or the rejection of the Inputs, Outputs, and Outcomes was performed based on the method presented in Figure 2.

Firstly the authors gave an initial classification to the Inputs, Outputs, and Outcomes; this classification was performed following peer-reviewing. The authors would discuss and

analyze each input, output, and outcome and decide the classification. This classification would only be given when the decision was unanimous by all the authors.

The final list of Inputs, Outputs, and Outcomes was later validated by the same method of peer-reviewing, where the authors discussed the list and then unanimously accepted it.

4. RESEARCH QUESTION

To answer the Research Questions previously mentioned, the authors created a method previously described to collect, analyze, and report the selected processes. The authors

identified all the processes explicitly described in the articles in the first step. Then, since there could be processes that were not explicitly described and therefore not identified, the authors analyzed the whole text, always trying to understand if it was possible to extract some processes throughout the text.

Along with the Processes, the authors also collected the Inputs, Outputs and, Outcomes. After identifying the Inputs, Outputs, and Outcomes, the authors followed the method summarised in Figure 2 to filter the relevant information from the unnecessary, achieving the final list of accepted Inputs, Outputs, and Outcomes.

This method consisted of a base classification of the Inputs, Outputs, and Outcomes. The authors would classify them by peer-reviewing as either:

- Merged (the Input/Output/Outcome was duplicated so the authors would classify them as such in order to merge them later);
- Removed (the Input/Output/Outcomes was considered out-of-scope and so was classified has removed to, later on, be removed from the list);
- Accepted (the Input/Output/Outcomes was considered as accepted and would be kept on the list).

After this first classification, the authors came up with the first validation of the Inputs, Outputs, and Outcomes. The authors would revise the Inputs, Outputs, and Outcomes to check if there were different classifications among authors. If there were, the authors discussed case by case until a unanimous decision was reached.

The result of this extraction is summarised in Table 3.

All the articles collected were analyzed and compared with each other. The rationale behind this phase was to merge equivalent processes but catalogued under different names. This process was iterative because all the processes were compared with the new process each time there was a merge.

In the last phase of this process, the authors analyzed what was found and reported it in this article. All Processes that were explicitly identified as such in their articles were kept in

the final table of Processes along with the definition given by the author (Table 3). This option was debated among the authors, but the final decision was to keep the Processes labelled and defined by the authors of each paper because since it is an SLR, we are only portraying what was found in the literature. For this reason, the authors do not agree with all the definitions, even going as far as to disagree on whether some of the reported processes are processes.

The authors noticed that several processes are referenced much more than the rest throughout this analysis phase. Therefore, it was decided to perform frequency analysis, represented in the column "Papers" of Table 3. The vast majority of articles refer mainly to two processes: Planning Management and Risk Management. The authors consider the Planning Management process is portrayed in the literature as the process that deals with elaborating a Business Continuity Plan, which leads it to be easily referenced in any article within this topic. However, the authors consider that this process might be too complex and extensive to be portrayed in a single process. Therefore, we recommend splitting this process into multiple processes. As for the Risk Management process, the authors consider it normal that it is one of the most addressed processes but find it strange the lack of references to the ISO 310xx standard when it is addressed.

5. PROCESS ASSESSMENT MODEL

In this section, the authors answer the remaining Research Questions (RQ1.2, RQ1.3, and RQ1.4).

The authors also decided to only present one complete process in this section (Table 4); however, the remaining processes are in Annex A.

In Table 4, the process (Planning Management) extracted from the literature with the Inputs, Outputs, and Outcomes is presented.

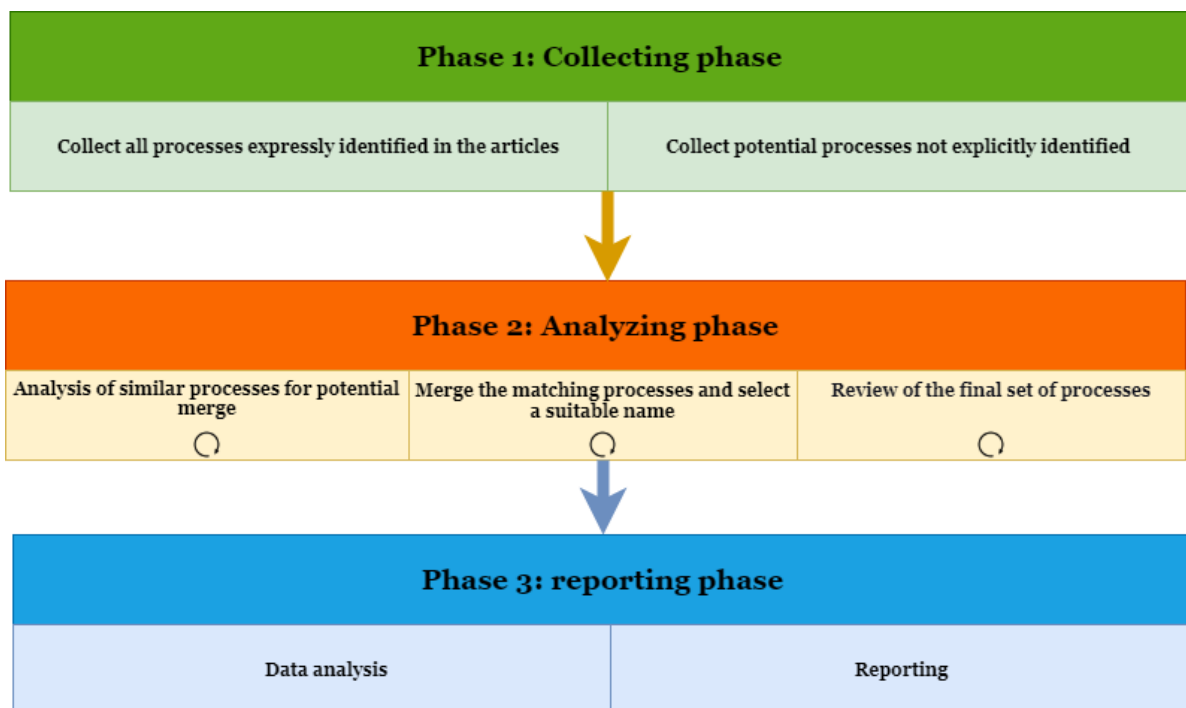


Figure 3. Method for consolidating the final list of processes

Table 4. Planning management process

Process ID	COM.01
Name	Planning Management
Purpose	Planning Management aims to ensure the organization's operations are secure and functional when even the worst-case scenario becomes a reality.
Outcomes	As a result of successful implementation of this process: 1. A business continuity plan is created [1, 7, 15, 24, 26, 29, 33, 35, 38, 39, 45]. 2. Approval from Executive Management is obtained [26]. 3. Competitive advantage after disruption is enhanced [20]. 4. Critical activities are identified and is ensured that essential functions continue during and after an incident [39]. 5. Effectiveness of mitigating business continuity risk is measured [43]. 6. Impact of risk is re-evaluated and reduced [16]. 7. A Back-up location with equipped backup systems is created [21]. 8. Organizational readiness is measured [43]. 9. Recovery point objectives are identified [35]. 10. Recovery requirements are identified [13]. 11. Recovery time objectives are identified [35]. 12. The current status and arrangement of the organization is evaluated [26].
Inputs	
BCMS objectives. [25, 33] BCMS scope [25, 33]. Business Impact Analysis. [29, 33, 35, 40, 41] Business strategy. [25] Capacity Plan. [25] Organization Policy. [40] BCMS stakeholders. [25] Recovery point objectives. [35] Risk register. [33, 40]	
Outputs	
Plans to anticipate and overcome disruptions. [21, 24, 29] List of BC plan stakeholders' roles and responsibilities. [27] Business Continuity Plan. [7, 15, 21, 24-26, 33, 35, 38, 39, 45] Capacity Plan. [25] List of dependencies between activities and processes. [25] Report evaluating the current status of the organization. [26] List of recovery requirements. [13]	

6. DISCUSSION

In this Systematic Literature Review, the authors gained an overview of what was present in the literature. After analyzing all the papers, the authors can group them into two different types. Some of the papers found defined the Processes explicitly and their Inputs, Outputs, and Outcomes. In these types of papers, the information was explicit and easy to deduce. The other type were papers where the Processes, Outcomes, Inputs, and Outputs were mixed in the information presented. The Processes, Inputs, Outputs, and Outcomes were retrieved from those papers after a deep analysis of each paper.

This process can be faulty due to the fact that, in some papers, the Processes were presented with different naming. The authors expected a Process to be universally known, but the same Process can be presented with a similar definition and a different naming in a different paper.

The authors use ISO 22301 [4] as a golden standard, for each time a Process was in doubt if it belonged in the scope of this work, an analysis and comparison with the ISO 22301 was performed.

Although the Systematic Literature Review was followed to gather the information needed, the model developed may be incomplete. As we can see in Table 3, some Processes are much more referenced than others, leading to some having more information. For example, in Table 4, the authors presented the Planning Management Process, along with this Process the authors identified twelve Outcomes present in the

literature. Meanwhile, other Processes like Prevention Management (Annex A) only had four Outcomes identified.

The gap mentioned in the previous paragraph comes from the literature. This gap arose a problem, some Processes are much more complete than others. Some processes could be incomplete, but processes that might be essential to the Process Assessment Model developed were not found in the literature—making these Processes absent from this Model.

During the literature analysis and the consequent check of the Processes found in the literature with the Processes present in the ISO22301 [4], the authors found that some Processes present in the ISO could not be found in the Literature. One of these Processes can be, for example, the Leadership Process.

The Leadership Process defines the roles of the top management in the organization. This was not a topic present in the Literature, and since this topic was not covered, the Process Assessment Model presented does not have the Leadership into consideration.

This model lacks scientific validation, which can be achieved by using the Delphi methodology and analyzing the reviews given by the participants. The authors can verify the Model in real organizations or set up meetings with expertise that can have valuable input to this work.

7. CONCLUSION

In this paper, a systematic literature review research was

performed to analyze the existing literature, identify the Business Continuity Maturity Models, and collect Business Continuity Management processes along with their Inputs, Outputs, and Outcomes. This research answered four Research Questions about the existing research literature. After analyzing the 39 papers, the researchers came up with a collection of Processes, inputs, outputs, and outcomes.

This collection of Business Continuity Management processes was structured after following the method shown in Figure 3 and culminated in the processes' list and their definitions in Table 3. This list of processes only represents what is defined as such in the literature. By analyzing this list, it was possible to conclude that most of the articles refer mainly to two processes: Planning Management and Risk Management.

To answer the remaining Research Questions, the authors followed the methodology in Figure 2. This methodology led to each Process having a final set of Inputs, Outputs, and Outcomes.

In this research, there were some limitations that we must point out. Although methods were used whenever possible, there is always a bias component in this type of investigation. In our case, the process of choosing articles as well as the merge process suffers from this limitation.

When analyzing the search string, the authors concluded that it could be improved to find more articles on the topic. The list of articles was not validated by experts and only represents what was found in the literature. Also, in this investigation, non-scientific reports were not considered, which could help understand the maturity of this topic in the industry.

As future work, we consider that the process list presented in this research should be validated. Besides, we acknowledge that comparing and mapping the results obtained in this investigation with the ISO 22301 standard [4] can benefit the field. This comparison could establish a bridge between the scientific and the business community. Finally, we suggest that linking and complementing interdependent business continuity management areas, such as risk management, security, and strategy, should be studied.

REFERENCES

- [1] Speight, P. (2011). Business continuity. *Journal of Applied Security Research*, 6(4): 529-554.
- [2] Randeree, K., Mahal, A., Narwani, A. (2012). A business continuity management maturity model for the UAE banking sector. *Business Process Management Journal*, 18(3): 472-492. <https://doi.org/10.1108/14637151211232650>
- [3] ISO, I. (2015). ISO/IEC 33004: 2015 Information technology—Process assessment—Requirements for process reference, process assessment and maturity models. International Organization for Standardization.
- [4] ISO. (2019). ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements.
- [5] Kitchenham, B., Brereton, O. P., Budgen, D., Turner, M., Bailey, J., Linkman, S. (2009). Systematic literature reviews in software engineering--a systematic literature review. *Information and Software Technology*, 51(1): 7-15. <https://doi.org/10.1016/j.infsof.2008.09.009>
- [6] ISO. (2019). Societal security — Business continuity management systems — Requirements (Vol. 2019).
- [7] Peterson, C.A. (2009). Business Continuity Management & guidelines. Proceedings of the 2009 Information Security Curriculum Development Annual Conference, InfoSecCD'09, pp. 114-120. <https://doi.org/10.1145/1940976.1940999>
- [8] Cerullo, V., Cerullo, M.J. (2004). Business continuity planning: A comprehensive approach. *Information Systems Management*, 21(3): 70-78. <https://doi.org/10.1201/1078/44432.21.3.20040601/82480.11>
- [9] Hersyah, M.H., Derisma. (2018). A Literature Review on Business Continuity Based on ISO 22301, Six Sigma and Customer Satisfaction Evaluation. 2018 International Conference on Information Technology Systems and Innovation, ICITSI 2018 - Proceedings, pp. 392-397. <https://doi.org/10.1109/ICITSI.2018.8696075>
- [10] ISO. (2016a). Technical Specification ISO / IEC TS 33052 Information technology — Process reference model (PRM) for information security management.
- [11] ISO. (2016b). Technical Specification ISO / IEC TS 33072 Information technology - Process assessment - Process capability assessment model for information security management.
- [12] Ajimoko, T. (2016). Business continuity management in a dynamic environment-lessons from Macondo. Society of Petroleum Engineers - SPE African Health, Safety, Security and Environment and Social Responsibility Conference and Exhibition 2016, pp. 386-393.
- [13] Alexander, A.G. (2020). A Methodology for Developing a Business Continuity Strategy. In 35.233.142.190. Retrieved October 14, 2020.
- [14] Armour, M. (2015). Talking about a (business continuity) revolution: Why best practices are wrong and possible solutions for getting them right. *Journal of business continuity & emergency planning*, 9(2): 103-111.
- [15] Aronis, S., Stratopoulos, G. (2016). Implementing business continuity management systems and sharing best practices at a European bank. *Journal of Business Continuity & Emergency Planning*, 9(3): 203-217.
- [16] Aziz, N.M.A.A., Jambari, D.I. (2019). Information Management Procedures for Business Continuity Plan Maintenance. In 2019 International Conference on Electrical Engineering and Informatics (ICEEI), pp. 489-495. <https://doi.org/10.1109/ICEEI47359.2019.8988804>
- [17] Baba, H., Watanabe, T., Miyata, K., Matsumoto, H. (2015). Area business continuity management, a new approach to sustainable local economy. *Journal of Disaster Research*, 10(2): 204-209. <https://doi.org/10.20965/jdr.2015.p0204>
- [18] Baba, H., Watanabe, T., Nagaishi, M., Matsumoto, H. (2014). Area business continuity management, a new opportunity for building economic resilience. *Procedia Economics and Finance*, 18(4th International Conference on Building Resilience, Incorporating the 3rd Annual Conference of the ANDROID Disaster Resilience Network, 8th-11th September 2014, Salford Quays, United Kingdom), pp. 296-303. [https://doi.org/10.1016/S2212-5671\(14\)00943-5](https://doi.org/10.1016/S2212-5671(14)00943-5)
- [19] Bajgoric, N. (2014). Business continuity management: A systemic framework for implementation. *Kybernetes*, 43(2): 156-177. <https://doi.org/10.1108/K-11-2013-0252>

- [20] Bakar, Z.A., Yaacob, N.A., Udin, Z.M. (2015). The effect of business continuity management factors on organizational performance: A conceptual framework. *International Journal of Economics and Financial Issues*, 5: 128-134.
- [21] Cassel, W.R. (2004). Assessing business continuity requirements. *IEEE Power Engineering Society General Meeting*, 1: 822-823.
- [22] Epstein, B., Khan, D.C. (2014). Application impact analysis: A risk-based approach to business continuity and disaster recovery. *Journal of Business Continuity & Emergency Planning*, 7(3): 230-237.
- [23] Faertes, D. (2015). Reliability of supply chains and business continuity management. *Procedia Computer Science*, 55: 1400-1409. <https://doi.org/10.1016/j.procs.2015.07.130>
- [24] Fani, S.V., Subriadi, A.P. (2019). Business continuity plan: examining of multi-usable framework. *Procedia Computer Science*, 161: 275-282. <https://doi.org/10.1016/j.procs.2019.11.124>
- [25] Gibb, F., Buchanan, S. (2006). A framework for business continuity management. *International Journal of Information Management*, 26(2): 128-141. <https://doi.org/10.1016/j.ijinfomgt.2005.11.008>
- [26] Heng, G.M. (2015). Business Continuity Management Planning Methodology. *International Journal of Disaster Recovery and Business Continuity*, 6: 9-16.
- [27] Herbane, B., Elliott, D., Swartz, E.M. (2004). Business Continuity Management: time for a strategic role? *Long Range Planning*, 37(5): 435-457. <https://doi.org/10.1016/j.lrp.2004.07.011>
- [28] Hill, R., Burgess, S. (2003). Issues in business continuity management. *Information Technology and Organizations - Trends, Issues, Challenges and Solutions: Proceedings of the 2003 Information Resources Management Association Conference*, pp. 287-289.
- [29] Iqbal, A., Widyawan, Mustika, I.W. (2016). COBIT 5 Domain Delivery, Service and Support mapping for Business Continuity Plan. *AIP Conference Proceedings*, 1746(1): 1. <https://doi.org/10.1063/1.4953970>
- [30] Bajgoric, N. (2006). Information technologies for business continuity: an implementation framework. *Information management & computer security*.
- [31] Kepenach, R.J. (2007). Business continuity plan design. In *Second International Conference on Internet Monitoring and Protection (ICIMP 2007)*, p. 27. <https://doi.org/10.1109/ICIMP.2007.11>
- [32] Kozina, M. (2009). COBIT-ITIL mapping for business process continuity management. *Central European Conference on Information and Intelligent Systems*, 113.
- [33] Labus, M., Despotović-Zrakić, M., Bogdanović, Z., Barać, D., Popović, S. (2020). Adaptive e-business continuity management: Evidence from the financial sector. *Computer Science and Information Systems*, 17(2): 553-580. <https://doi.org/10.2298/CSIS190202037L>
- [34] Lindstrom, J., Samuelsson, S., Hagerfors, A. (2010). Business continuity planning methodology. *Disaster Prevention and Management*, 19(2): 243-255. <https://doi.org/10.1108/09653561011038039>
- [35] Tammineedi, R.L. (2010). Business continuity management: A standards-based approach. *Information Security Journal: A Global Perspective*, 19(1): 36-50. <https://doi.org/10.1080/19393550903551843>
- [36] Niemimaa, M. (2015). Interdisciplinary review of business continuity from an information systems perspective: Toward an integrative framework. *Communications of the Association for Information Systems*, 37: 69-102. <https://doi.org/10.17705/1CAIS.03704>
- [37] Nijaz, B., Mario, S., Lejla, T. (2011). Implementation of the IT governance standards through business continuity management: Cases from Croatia and Bosnia-Herzegovina. In *Proceedings of the ITI 2011, 33rd International Conference on Information Technology Interfaces*, pp. 43-50.
- [38] Takeshi, I., Hideaki, O., Tetsuya, Y. (2007). Fujitsu's Business Continuity Plan Development Methodology. *Fujitsu Scientific and Technical Journal*, 177: 168-177.
- [39] Păunescu, C. (2017). How prepared are small and medium sized companies for business continuity management? *Quality - Access to Success*, 18(161): 43-48.
- [40] Pramudya, G.W., Fajar, A.N. (2019). Business continuity plan using ISO 22301:2012 in IT solution company (pt. ABC). *International Journal of Mechanical Engineering and Technology*, 10(2): 865-872.
- [41] Rejeb, O., Bastide, R., Lamine, E., Marmier, F., Pingaud, H. (2012). A model driven engineering approach for business continuity management in e-Health systems. *2012 6th IEEE International Conference on Digital Ecosystems and Technologies (DEST), Digital Ecosystems Technologies (DEST), 2012 6th IEEE International Conference on*, pp. 1-7. <https://doi.org/10.1109/DEST.2012.6227931>
- [42] Sambo, F., Bankole, F.O. (2016). A Normative Process Model for ICT Business Continuity Plan for Disaster Management in Small, Medium and Large Enterprises. *International Journal of Electrical & Computer Engineering (2088-8708)*, 6(5): 2425.
- [43] Strong, B. (2010). Creating meaningful business continuity management programme metrics. *Journal of Business Continuity & Emergency Planning*, 4(4): 360-367.
- [44] Suresh, N., Sanders, G.L., Braunscheidel, M.J., Suresh, N., Sanders, G.L., Braunscheidel, M.J. (2020). Business continuity management for supply chains facing catastrophic events. *IEE Engineering Management Review*, 48(3): 129-138. <https://doi.org/10.1109/EMR.2020.3005506>
- [45] Svata, V. (2013). System View of Business Continuity Management. *Journal of Systems Integration (1804-2724)*, 4(2): 19.
- [46] Winkler, U., Fritzsche, M., Gilani, W., Marshall, A. (2010). A model-driven framework for process-centric business continuity management. *2010 Seventh International Conference on the Quality of Information and Communications Technology, Quality of Information and Communications Technology (QUATIC), 2010 Seventh International Conference*, pp. 248-252. <https://doi.org/10.1109/QUATIC.2010.46>

ANNEXE

Process ID	
Name	Risk Management
Purpose	Risk Management ensures the identification of risks and disruptions to the organization's prioritized activities, systematically analyze risk, evaluate which disruption related risks have required treatment and, identifies treatments commensurate with business continuity objectives
Outcomes	<p>As a result of successful implementation of this process:</p> <ol style="list-style-type: none"> 1. Potential threats to an organization and the possible impacts of these threats to business operations are identified. (C. Suresh et al., 2020) 2. Risk is accepted or rejected. (Hill & Burgess, 2003) 3. Risk is analyzed. (Labus et al., 2020) (Aronis & Stratopoulos, 2016) (Păunescu, 2017) 4. Risk is assessed. (Hill & Burgess, 2003) (Heng, 2015) (Svata, 2013) (Forbes Gibb & Buchanan, 2006) 5. Risk is avoided, transfered or reduced to acceptable level. (Hill & Burgess, 2003) (Bakar et al., 2015) (C. Suresh et al., 2020) (Aziz & Jambari, 2019) (Aronis & Stratopoulos, 2016) (Svata, 2013) 6. Risk is evaluated. (Aronis & Stratopoulos, 2016) (Labus et al., 2020) (Nijaz et al., 2011) (Forbes Gibb & Buchanan, 2006) (Hitoshi Baba et al., 2014) (C. Suresh et al., 2020) 7. Risk is identified and ways to mitigate are proposed. (Kepenach, 2007) (Aronis & Stratopoulos, 2016) (C. Suresh et al., 2020) (Ajimoko, 2016) (Aziz & Jambari, 2019) (Forbes Gibb & Buchanan, 2006) (Sambo & Bankole, 2016) (Lingeswara Tammineedi, 2010) (Păunescu, 2017) 8. Risk Scenario and Business impact are analyzed. (Hitoshi Baba et al., 2014) (H Baba et al., 2015) (Heng, 2015)
Inputs	
<p>Application architecture (Forbes Gibb & Buchanan, 2006).</p> <p>Business Impact Analysis (Strong, 2010) (Svata, 2013) (Forbes Gibb & Buchanan, 2006) (Labus et al., 2020).</p> <p>List of necessary resources for key business processes (Labus et al., 2020).</p> <p>Process map and workflows. (Forbes Gibb & Buchanan, 2006).</p> <p>BCMS objectives (Labus et al., 2020) (Forbes Gibb & Buchanan, 2006).</p> <p>BCMS stakeholders. (Forbes Gibb & Buchanan, 2006).</p> <p>BCMS scope. (Labus et al., 2020) (Forbes Gibb & Buchanan, 2006).</p>	
Outputs	
<p>Risk Assessment, Control and Monitoring report. (Svata, 2013) (C. Suresh et al., 2020) (Păunescu, 2017) (Fani & Subriadi, 2019) (Aronis & Stratopoulos, 2016) (Heng, 2015) (Hill & Burgess, 2003) (Aziz & Jambari, 2019)</p> <p>Report with the avoided risks, transferred risks or reduced risks to acceptable level. (Hill & Burgess, 2003) (Lingeswara Tammineedi, 2010) (Aziz & Jambari, 2019) (Nijaz et al., 2011) (Sambo & Bankole, 2016) (C. Suresh et al., 2020)</p> <p>Report with the assess of the cost and effectiveness of risk controls. (Heng, 2015) (Sambo & Bankole, 2016)</p> <p>Business Impact Analysis. (Sambo & Bankole, 2016) (Hitoshi Baba et al., 2014) (Lingeswara Tammineedi, 2010) (Heng, 2015) (Randeree, Mahal, et al., 2012) (Kepenach, 2007) (Speight, 2011)(Aronis & Stratopoulos, 2016)</p> <p>Risk Register. (Hitoshi Baba et al., 2014) (C. Suresh et al., 2020) (Sambo & Bankole, 2016) (Lingeswara Tammineedi, 2010) (Păunescu, 2017) (Forbes Gibb & Buchanan, 2006) (Fani & Subriadi, 2019) (Aronis & Stratopoulos, 2016) (Speight, 2011)(Aziz & Jambari, 2019) (Nijaz et al., 2011) (Labus et al., 2020) (H Baba et al., 2015)</p> <p>Risk policies. (Aziz & Jambari, 2019)</p>	

Process ID	
Name	Exercising and testing
Purpose	Exercise and Testing ensures that the business continuity procedures are consistent with its business continuity objectives
Outcomes	<p>As a result of successful implementation of this process:</p> <ol style="list-style-type: none"> 1. Measurement criteria is developed. (Forbes Gibb & Buchanan, 2006) 2. Narrative scenarios are executed. (Aronis & Stratopoulos, 2016) 3. Plans are tested. (Aronis & Stratopoulos, 2016) 4. Staff is debriefed. (Forbes Gibb & Buchanan, 2006)

	5. Testing plan is developed and designed. (Forbes Gibb & Buchanan, 2006) (Heng, 2015) 6. Tests are conducted and the results are assessed and corrected. (Forbes Gibb & Buchanan, 2006) (Heng, 2015)
Inputs	
Business Continuity Plan. (Forbes Gibb & Buchanan, 2006)	
BCMS objectives. (Labus et al., 2020) (Forbes Gibb & Buchanan, 2006)	
BCMS stakeholders(Forbes Gibb & Buchanan, 2006)	
BCMS scope. (Labus et al., 2020) (Forbes Gibb & Buchanan, 2006)	
Report with the avoided risks, transferred risks or reduced risks to acceptable level. (Forbes Gibb & Buchanan, 2006)	
Outputs	
Report with the Test Program. (Heng, 2015)	
Test report. (Forbes Gibb & Buchanan, 2006)	

Process ID	
Name	Implementation Management
Purpose	Implementation Management ensures to put in place any improvements to operating procedures, infrastructure, security, etc., which can help to transfer, minimize or absorb the risks of processes and services being compromised
Outcomes	As a result of successful implementation of this process: 1. Backup copies of their critical data, paper or electronic are stored at alternate sites. (Randeree, Mahal, et al., 2012) 2. Costs and resources utilization are tracked. (Forbes Gibb & Buchanan, 2006) 3. Disaster recovery plans are implemented. (Forbes Gibb & Buchanan, 2006) 4. Risk management strategies are implemented. (Forbes Gibb & Buchanan, 2006) 5. The impact of the identified risks are reduced and mitigated. (Rejeb et al., 2012) 6. Development, compilation and maintenance of procedures on incidents (Rejeb et al., 2012)
Inputs	
Organization Policy. (Forbes Gibb & Buchanan, 2006)	
Business Impact Analysis (Forbes Gibb & Buchanan, 2006)	
Business Continuity Plan. (Forbes Gibb & Buchanan, 2006)	
Information strategy. (Forbes Gibb & Buchanan, 2006)	
Infrastructure descriptions (architectures, configurations floor-plans, inventory, etc.). (Forbes Gibb & Buchanan, 2006)	
Regulators' codes of practice. (Forbes Gibb & Buchanan, 2006)	
Report with the avoided risks, transferred risks or reduced risks to acceptable level. (Forbes Gibb & Buchanan, 2006)	
Outputs	
Report with the results of testing the BC plan. (Fani & Subriadi, 2019)	
Implementation report. (Forbes Gibb & Buchanan, 2006)	

Process ID	
Name	Prevention Management
Purpose	Prevention Management ensures the identification of an organization's exposure to internal and external threats and synthesizes hard and soft assets to provide effective prevention and recovery.
Outcomes	As a result of successful implementation of this process: 1. A collection of procedures for the various business units to ensure the continuance of critical business processes is developed. (Randeree, Mahal, et al., 2012) 2. A strategy to prevent threats is created (Randeree, Mahal, et al., 2012) 3. Organization's exposure to internal and external threats is identified. (Herbane et al., 2004) (Winkler et al., 2010) 4. Conformity of the impact of disasters/disruptions is determined. (Randeree, Mahal, et al., 2012)
Inputs	
Risk Register. (Winkler et al., 2010)	

Business Impact Analysis (Winkler et al., 2010)
Outputs
Assessment of the business impact of threats. (Winkler et al., 2010)
List of internal and external threats to the organization. (Herbane et al., 2004) (Winkler et al., 2010)
Report with strategies and responses to threats and crisis events. (Winkler et al., 2010) (Randeree, Mahal, et al., 2012)

Process ID	
Name	Impact and Recovery Management
Purpose	Impact and Recovery Management ensures the protection of the prioritized activities, mitigates, responds and manages impacts
Outcomes	As a result of successful implementation of this process: <ol style="list-style-type: none"> 1. Monitoring and control mechanisms are established. (Forbes Gibb & Buchanan, 2006) 2. Programme scope, roles, responsibilities and processes are defined and agreed. (Forbes Gibb & Buchanan, 2006) 3. Conformity of risks are determined. (Kozina, 2009) 4. Guidelines for conducting BCM are identified and specified. (Forbes Gibb & Buchanan, 2006)
Inputs	
	Organization Policy. (Forbes Gibb & Buchanan, 2006)
	Capacity Plan. (Forbes Gibb & Buchanan, 2006)
	Framework for establishing and maintaining the business continuity capability of an organization. (Forbes Gibb & Buchanan, 2006)
Outputs	
	List of agreed key processes. (Forbes Gibb & Buchanan, 2006)
	Checklist of key external regulatory issues. (Forbes Gibb & Buchanan, 2006)
	Plans for restoring business activities in case of disaster. (Kozina, 2009)
	Resource allocation and accounting procedures. (Forbes Gibb & Buchanan, 2006)
	Report with the review cycles and procedures. (Forbes Gibb & Buchanan, 2006)

Process ID	
Name	Mitigation Management
Purpose	Mitigation Management ensures the testing of the risk mitigation strategies, and the disaster recovery plans are carried out both regularly and comprehensively to see whether the plans are still relevant and deliverable.
Outcomes	As a result of successful implementation of this process: <ol style="list-style-type: none"> 1. The business units' resources are identified and mobilized. (Heng, 2015) 2. Emergency response teams are created. (Forbes Gibb & Buchanan, 2006) 3. BCP is analyzed with the Mitigation Management objectives. (Aziz & Jambari, 2019) 4. Risk mitigation strategies are tested according to risk mitigation objectives. (Forbes Gibb & Buchanan, 2006)
Inputs	
	List of goals for business continuity. (Heng, 2015)
	Capacity Plan (Forbes Gibb & Buchanan, 2006)
	Business Impact Analysis. (Heng, 2015)
	Process map and workflows. (Forbes Gibb & Buchanan, 2006)
	BCMS objectives. (Labus et al., 2020) (Forbes Gibb & Buchanan, 2006)
	BCMS participants (Forbes Gibb & Buchanan, 2006)
	BCMS scope. (Labus et al., 2020) (Forbes Gibb & Buchanan, 2006)
Outputs	
	Document about the testing of the disaster recovery plans. (Forbes Gibb & Buchanan, 2006)

Emergency response teams. (Forbes Gibb & Buchanan, 2006)
Risk mitigation strategies. (Forbes Gibb & Buchanan, 2006)

Process ID	
Name	Requirements Management
Purpose	Requirements Management ensures the analysis of business continuity requirements based on the data that supports the action plan development.
Outcomes	As a result of successful implementation of this process: 1. The goals for business continuity are listed (Takeshi et al., 2007)
Inputs	
BCMS scope. (Labus et al., 2020)	
List of goals for business continuity. (Forbes Gibb & Buchanan, 2006) (Labus et al., 2020)	
Capacity Plan. (Forbes Gibb & Buchanan, 2006) (Labus et al., 2020)	
Business Impact Analysis (Labus et al., 2020)	
Risk Register. (Labus et al., 2020)	
Report with the avoided risks, transferred risks or reduced risks to acceptable level. (Forbes Gibb & Buchanan, 2006)	
Risk Assessment, Control and Monitoring report. (Forbes Gibb & Buchanan, 2006)	
Outputs	
List of goals for business continuity (Takeshi et al., 2007).	

Process ID	
Name	Strategy Support
Purpose	Strategy Support ensures that the organization determines and provides the resources needed for the establishment, implementation, maintenance and continual improvement of the Business Continuity Management Strategy.
Outcomes	As a result of successful implementation of this process: 1. Crisis organization is established. (Peter Speight, 2011) 2. Planned assignment of tasks. (Peter Speight, 2011) 3. Information Strategy is developed.
Inputs	
Business Impact Analysis. (Pramudya & Fajar, 2019)	
Organization Policy. (Pramudya & Fajar, 2019)	
Risk register. (Pramudya & Fajar, 2019)	
Outputs	
Capacity Plan.	

Process ID	
Name	Monitoring
Purpose	Monitoring ensures to determine what needs to be measured, the methods for monitoring, when the monitoring and measuring shall be performed and when the results shall be analyzed and evaluated.
Outcomes	As a result of successful implementation of this process: 1. The plan is trained, rehearsed and reviewed to ensure it stays up-to-date. (Rejeb et al., 2012)
Inputs	
Business Continuity Plan.	
Outputs	
Documentation Test Result. (Fani & Subriadi, 2019)	
Report with periodic reviews (Fani & Subriadi, 2019)	
Recording of Findings. (Fani & Subriadi, 2019)	

Process ID	
Name	Policy Management

Purpose	Policy Management ensures that a business continuity policy is established that is appropriate to the purpose of the organization, provides a framework for setting business continuity objectives, includes a commitment to satisfy applicable requirements
Outcomes	As a result of successful implementation of this process: 1. Establishing and maintaining the business continuity capability of an organization. (Lingeswara Tammineedi, 2010)
Inputs	
Outputs	
Framework for establishing and maintaining the business continuity capability of an organization. (Lingeswara Tammineedi, 2010)	
Organization Policy. (Business Continuity Strategy) (Aziz & Jambari, 2019)	