


---

# Towards a Comprehensive Framework for the Multidisciplinary Evaluation of Organizational Maturity on Business Continuity Program Management: A Systematic Literature Review

Nelson Russo <sup>a</sup>, Leonilde Reis <sup>b</sup>, Clara Silveira <sup>c</sup>, and Henrique S. Mamede <sup>d</sup>

<sup>a</sup>School of Science and Technology, University of Trás-os-Montes and Alto Douro, Real, Portugal; <sup>b</sup>School of Business Administration, Polytechnic Institute of Setúbal, Setúbal, Portugal; <sup>c</sup>School of Technology and Management, Polytechnic Institute of Guarda, Guarda, Portugal; <sup>d</sup>Department of Science and Technology, Universidade Aberta, Lisbon, Portugal

## ABSTRACT

Organizational dependency on Information and Communication Technology (ICT) drives the preparedness challenge to cope with business process disruptions. Business Continuity Management (BCM) encompasses effective planning to enable business functions to resume to an acceptable state of operation within a defined timeframe. This paper presents a systematic literature review that communicates the strategic guidelines to streamline the organizational processes in the BCM program, culminating in the Business Continuity Plan design, according to the organization's maturity. The systematic literature review methodology follows the Evidence-Based Software Engineering protocol assisted by the Parsifal tool, using the EbscoHost, ScienceDirect, and Scopus databases, ranging from 2000 to February 2021. International Standards and Frameworks guide the BCM program implementation, however, there is a gap in communicating metrics and what needs to be measured in the BCM program. The major paper result is the confirmation of the identified gap, through the analysis of the studies that, according to the BCM components, report strategic guidelines to streamline the BCM program. The analysis quantifies and discusses the contribution of the studies on each BCM component to design a framework supported by metrics, that allows assessing the organization's preparedness in each BCM component, focusing on Information Systems and ICT strategies.

## KEYWORDS

Business continuity plan; information and communication technology; information systems; measurement; organizational maturity

## 1. Introduction

Information and Communication Technologies (ICT) are nowadays strategic in every organization and, although, on different levels of dependence, the need for information flow is essential. Not protecting information, or worse, losing it, can be critical to an organization's survival. In this context, organizations must prepare for the eventuality of interruptions in their business processes, especially those supported by ICT services.

Industry 4.0, is empowered by the seamless collaboration of communication technology (CT), information technology (IT), and operation technology (OT), i.e., CIOT collaboration. The OT domain encompasses all the industrial elements. The CT domain is represented by various wired/wireless and long-/short-distance communication standards and technologies. The IT domain is the platform that realizes the unified collection,

storage, and analysis of the data collected by workers or sensor networks from the OT domain. It is empowered, for example, by advanced cloud computing, digital twin, and Artificial Intelligence (Wan et al., 2022).

In the context of ICT, the challenging uncertainties in the global economy, or the new hazards and threats emerging from climate change, military conflicts, or pandemic and post-pandemic affects the BCM and BCP and require strategies that urge implementation in practice.

However, processes related to risk management are relegated to the background. The absence of a consistent approach to risk management can lead to many undesirable outcomes and, ultimately, to a decrease in operational efficiency and effectiveness (Varajão & Amaral, 2021). Preparation and planning are the key and project management is the door to allow the organization to step into the world of

---

resilience (Kliem & Richie, 2016). In this context, Business Continuity (BC) is the strategic and tactical organizational capability to plan and respond to business disruptions (Ramakrishnan & Viswanathan, 2011) in order to continue business operations at an acceptable pre-defined level. Business Continuity Management (BCM) is a management process of implementing and maintaining BC (ISO 22301, 2019) that, among others, incorporates Risk Management (Torabi et al., 2016), to identify potential intentional and unintentional threats to an organization. It aims to develop the organization's ability to respond to these threats.

In this context, Organizational Resilience is the ability of an organization to absorb and adapt in a changing environment (ISO 22316, 2017), while resilience has many meanings according to the context. For example, resilience is the ability of a system to recover operational condition quickly following an incident (ISO/IEC 22989, 2022). Is the capacity to withstand failure in one or more of the ICT equipment or Datacenter infrastructures (ISO/IEC TS 22237-3, 2022) or even the ability to recover from security compromises or attacks (ISO/IEC 29180, 2012).

Technology, people, and processes are exposed to threats and are the three fundamental aspects of the BCM approach (Mansol et al., 2015). Therefore, there are benefits in implementing the BCM program (Russo & Reis, 2020b).

Thus, a BC Plan (BCP) is designed to avoid or mitigate risks; reduce the impact of crisis or disaster conditions and reduce the time needed to

restore conditions to a normal operating state (Cerullo & Cerullo, 2004). Consequently, BCM is more than Risk Management, and other components of BCM must be managed effectively to provide a BCP. Therefore, to design a BCP, it is necessary to understand each of the activities of the BCM and acquire the organization's commitment to improve and prioritize program development activities (Isa et al., 2019). However, to plan operations, it is necessary to understand the Organization and its vital business processes. It is essential to understand the information flows, the supporting Information Systems (IS), and the expected recovery times, in order to understand the ICT capacity for recovery and restoration of the business (Russo & Reis, 2020a).

In this context, organizations can select from a variety of International Standards and Frameworks, hereinafter identified as Frameworks that guide the design, implementation, and maintenance of a comprehensive BCM. The different perspectives of the Framework for BCM define a set of requirements, practices, or activities, which aim to manage the identified BCM components. Figure 1 presents the essential components of the BCM, according to the Frameworks and the design methodology of a BCP (Russo & Reis, 2020b). It should start with obtaining the administration support for the BCM Program and creating the BC Teams to initiate Organization Understanding activities.

Figure 1 shows the sequence of actions and the interrelationship of the BCM components. Using

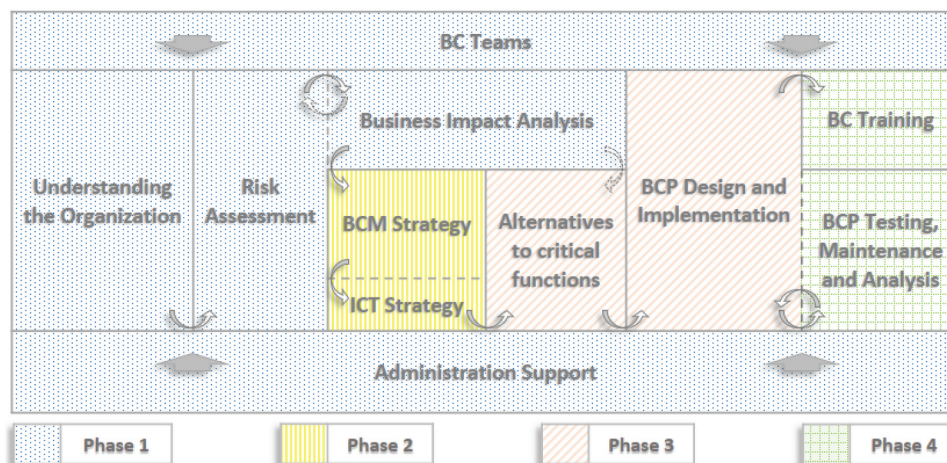


Figure 1. BCM components. Source: adapted from (Russo & Reis, 2020b).

unique patterns and colors, the phasing in time is represented in the methodological approach for designing and maintaining a BCP. This suggests the set of components that must be completed to start another phase. For example, the context establishment in the information security risk management process (ISO/IEC 27005, 2018) is expected to be conducted along the “Understanding the Organization” activities as input for Risk Assessment. The Risk Treatment (ISO/IEC 27005, 2018) activities are conducted in the Phase 2 activities and in the “Alternatives to critical functions.”

Some organizations postpone the implementation of BCP because of restrictions on its design. It can be justified by technical or financial reasons or by the interpretation of requirements (Russo & Reis, 2020c), or restrict company policies and time constraints to complete the project (Fani & Subriadi, 2019). These constraints reveal the perceived complexity to start the BCM program and the specialized knowledge for designing and

implementing a BCP and its maintenance (Wong, 2009). To address constraint mitigation, there is a need to understand each identified BCM component of the BCM System (BCMS). A literature review can reveal a larger set of constraints and strategic guidelines to streamline the BCP design. To identify the research areas the Frameworks were compared, resulting in a set of areas not formally covered by those references. Figure 2 maps, in the outer slices, the preeminent activities that are addressed in the Frameworks. A non-red shape means that the activities are defined formally in the Framework. The preliminary gaps in the formal definition of activities in each common component of BCM are mapped as red shapes in the outer slices, according to the Framework referenced by the legend.

Figure 2 highlights the identified gaps, such as the constitution of BC Teams and the suggestion of metrics that allow inferring the maturity of the BCM program in the organization. It is intended

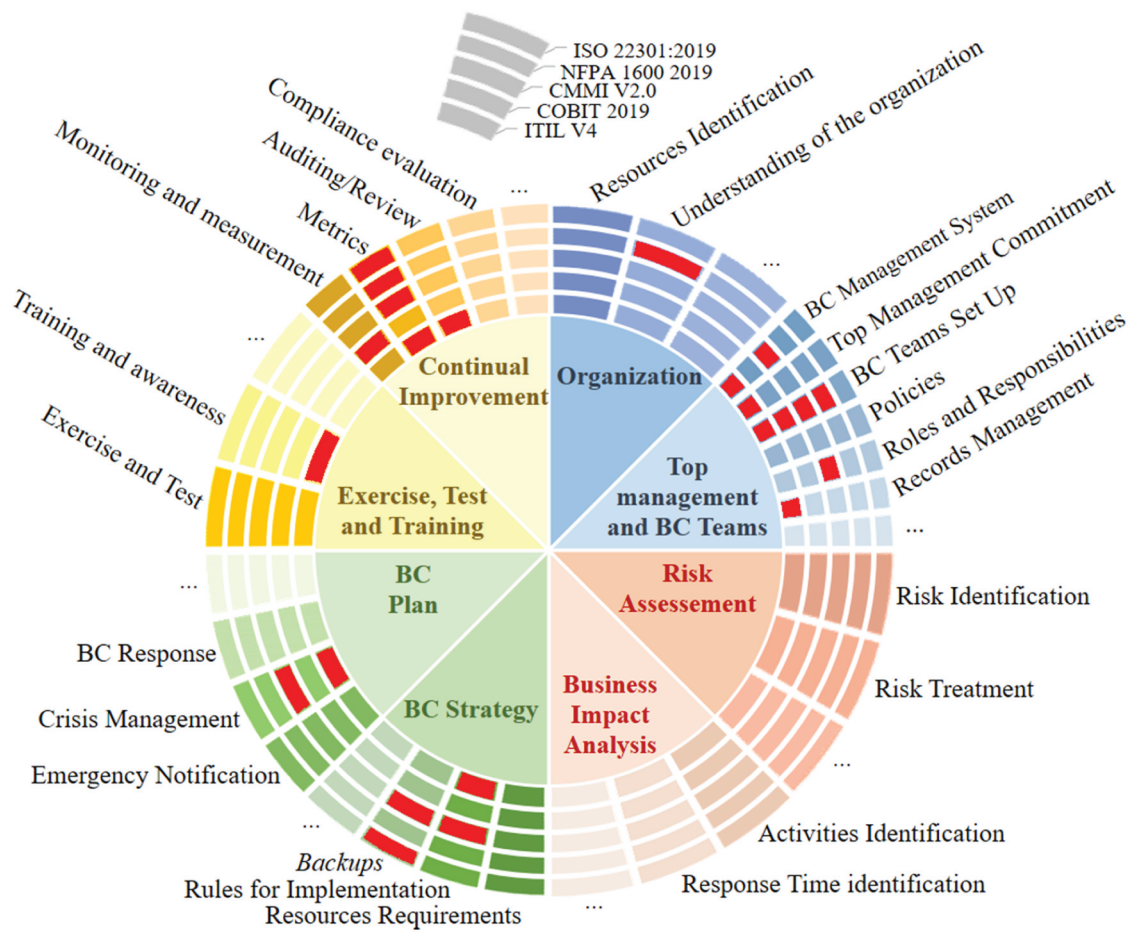


Figure 2. BCM components, relevant activities, and gap analysis. Source: adapted from (Russo et al., 2021).

to argue that, despite the complexity and pertinence of the reviewed Frameworks, there is an open opportunity to address the gap associated with defining BC metrics. While the Frameworks guidance focuses on the methods to be used, when, and by whom, its guidelines indicate that organizations must determine what needs to be measured.

Maturity models are used to assess current situations, guide improvement initiatives, and track progress (Röglinger et al., 2012). An organization's process maturity can be explained as a measure of an organization's readiness and capability expressed through its people, processes, data, and technologies. The consistent measurement practices that are in place identify the degree to which processes are formally defined, managed, flexible, measured, and effective (Fryt, 2019). Therefore, maturity models typically include a sequence of levels that form an anticipated, desired, or logical path from an initial state to maturity (Röglinger et al., 2012). A maturity level is a classification that describes the degree to which organizational processes meet the intent of a collection of similar practices. The ranking is based on achieving a specific set of practice group levels.

Therefore, the higher the organization's maturity level, the better its performance in planning mitigation activities (CMMI Institute, 2018), and in maintaining the information documented in a BCP.

In this context, one of the success factors in the development of the BCM strategy is the definition of performance measures to identify the minimum operational service levels, such as availability, reliability, or responsiveness (Hibberd, 2011). Organizations benefit from this achievement and from the existence of a framework that guides business disruption mitigation, BCP design, and BCM program activities. From a benefits management perspective, metrics can support the verification of business value and validation of the project's success (PMI, 2017). The evaluation of success, in addition to the associated costs, is beneficial to the organization. It allows the understanding of the project and the identification of opportunities for improvement, alerting to weaknesses in project management. In addition, it provides details on the successful implementation of management, such as when the assessment process

can be defined. Also, details on which criteria can be defined, who should participate in the assessment, when the assessment should take place, among other aspects (Pereira et al., 2021).

The BC maturity assessment allows the organization to assess its BC performance, program implementation, or current capability in a specific BCM activity. This activity assessment can comprise a sequence of levels, which forms a logical path to BCM component maturity. A set of metrics can measure each level, showing the organization's ability in a particular BCM activity. The Systematic Literature Review (SLR) identifies studies that use frameworks, models, and other contributions that address the main areas of interest reported in this article. The main objective of this work is to present the SLR that synthesizes the existing evidence for the identification of possible gaps in the literature, providing ways to answer the research question.

This paper is organized into six sections: the first section introduces the major concepts, research motivation, and problem identification. The second section presents the overview of the Frameworks and in the third section, the research methodology. The fourth section highlights the areas reported in the SLR studies and explores their contributions, according to the research question, also suggesting the research contribution and limitations. The fifth section presents the findings and discusses the SLR process. The conclusion is in the sixth section.

## 2. Frameworks overview

Since the motivation for this research is derived from the analysis of some Frameworks, it is relevant to present them. The International Organization for Standardization (ISO) has published the ISO 22301:2019, specifying requirements for implementing, maintaining, and improving a management system. It aims to protect, reduce the likelihood of occurrence, prepare, respond and recover from disruptions when they arise (ISO 22301, 2019).

The Capability Maturity Model Integration (CMMI) V2.0 is a set of best practices that allow companies to improve performance and propose planning mitigation activities to deal with significant disruptions in business



operations (CMMI Institute, 2018). The Control Objectives for Information and related Technology (COBIT) provides a framework for enterprise ICT governance and management. In this research context, the main objective of COBIT 2019 is to provide a plan to enable companies and ICT organizations to respond to incidents and adapt quickly to outages (ISACA, 2018). The Information Technology Infrastructure Library (ITIL) offers a set of best practices. The ITIL 4 release provides guidance for tackling service management challenges and harnessing the potential of modern technology. It presents the Service Continuity Management Practices to guarantee the availability and performance of a service, in case of a disaster (ITIL, 2019). The National Fire Protection Association (NFPA) 1600 standard provides fundamental criteria for preparedness and resilience through a program that addresses prevention, mitigation, response, continuity, and recovery (NFPA, 2019).

These frameworks are structured into activities, objectives, or practices. They present their vision of the appropriate way to approach, guide, reduce, mitigate, face, or respond to disasters, incidents, or interruptions in business operations or in the delivery of services. These identified structures guide the assessment of the

areas in the literature review, represented in Figure 8.

### 3. Methodology

Literature reviews can serve as a basis for knowledge development and support new directions in a given field. Therefore, following an SLR methodology is relevant to create the bases to achieve the solution objectives (Hevner et al., 2004). The SLR should have predetermined targets and eligibility criteria, perform data extraction and assess the risk of bias (Young et al., 2014). Despite considering PRISMA-P (Moher et al., 2015) and ROSES (Haddaway & Macura, 2018) protocols, the SLR follows the guidelines provided by Evidence-Based Software Engineering (EBSE) (Kitchenham, 2004), with the help of the online tool Parsifal. An SLR is a research methodology characterized by being a transparent and reproducible way of analyzing existing literature (Cook et al., 1997). It is a prerequisite for a quantitative meta-analysis, summarizing existing evidence, and identifying any gaps in current research. It must specify how the researcher conducted the review and what types of records were reviewed. The SLR process adopted (Kitchenham, 2004) involves three main phases: planning, conducting, and reporting the review. Its stages are presented in Figure 3.

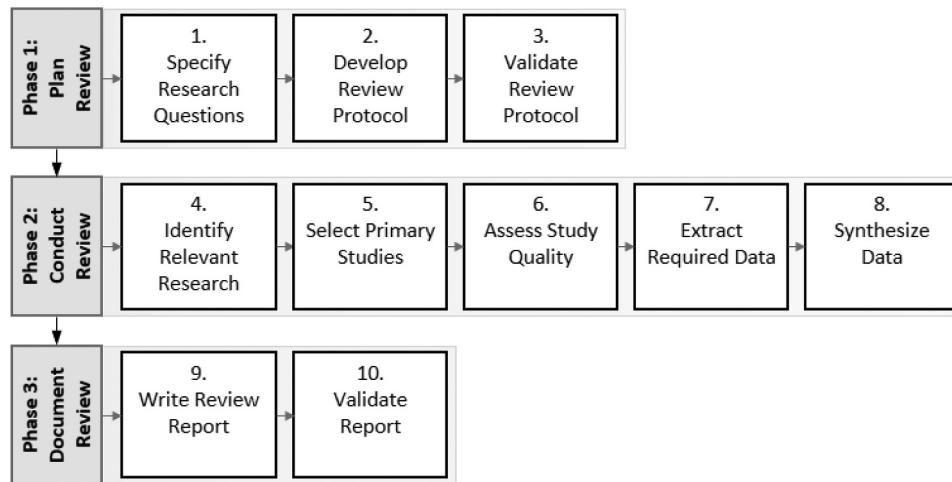


Figure 3. Systematic literature review process. Source: adapted from (Brereton et al., 2007).

Figure 3 represents the flow of the SLR process, which follows three essential steps of the EBSE practice (Brereton et al., 2007). First, convert the need for information into an answerable question. Secondly, find the best evidence with which to answer the question. The third step is to critically appraise the evidence for its validity (closeness to the truth), impact (size of the effect), and applicability (usefulness).

### 3.1. Research question

All research projects are dependent on the research question and available resources. Its formulation should identify the existing foundations for the work and clarify where the proposed research fits into the current body of knowledge (Kitchenham, 2004). The Population-Intervention-Comparison-Outcome-Context (PICOC) protocol was used. The proposed intervention is the design of a framework providing “strategic guidelines for the implementation of the business continuity plan.” Organizations are the population affected by the intervention, contextualized in organizations with business processes supported by ICT. The proposed interventional framework will be compared with other frameworks returned from

the SLR. The expected outcome is to support and streamline organizational processes for defining strategic guidelines for implementing a BCP, according to the organization’s maturity.

Hence, complying with stage 1 presented in Figure 3, the question to be answered is: “Is it possible to support an organization and to streamline its organizational processes, with the definition of strategic guidelines for implementing a BCP, which allows the formulation of response, restart, recovery and restoration of business processes, supported by ICT, at a pre-defined level of operability, according to the maturity and capacity of the organization?”

### 3.2. Review protocol development

The primary SLR purpose is to identify the BCM components, communicated throughout the last years. It is also a purpose to gather a set of strategic guidelines that complement the Frameworks, for each of the BCM components, aiming to streamline the BCP design.

In March 2021, the SLR was completed using the EbscoHost, ScienceDirect, and Scopus databases. The identification criteria to include publications in the review are presented in Figure 4.

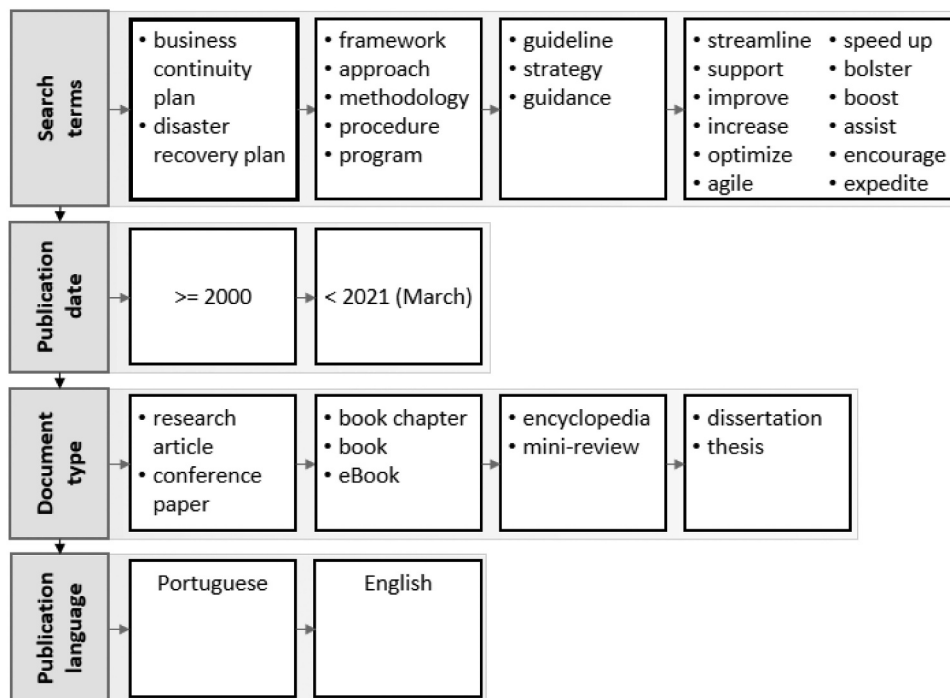


Figure 4. Publication identification criteria.

Figure 4 presents the primary search terms: “business continuity plan” or “disaster recovery plan.” These search terms were combined with “framework,” “guideline,” and “streamline,” along with a set of synonyms. The publication must have any of the search terms in the title, abstract, or keywords to be included in the review. The publication date ranges from 2000 (to be reasonably comprehensive) to February 2021. Nonetheless, for reporting and synthesis of the current body of knowledge, we decided to consider publications after 2015.

#### 4. Research analysis

The primary search returned 10,356 publications. Applying the identification criteria, resulted in 1240 potentially eligible publications. 14 publications were manually added since they did not fit the search string criteria, although highly cited in BCM papers. Figure 5 presents more details, from the initial eligible 1254 publications to the extracted 393 unique intervention studies used in this review.

Various types of bias can be refined in the quality assessment by considering specific items, such as the use of outcome measures inappropriate for answering the research question (Kitchenham, 2004). After title and abstract review, and full-text reading in some cases, for applying the inclusion or

exclusion criteria, 1254 articles were fully reviewed for potential inclusion and 856 were excluded.

A publication was excluded if it did not communicate strategic guidelines to design a BCP or if it was too specific to a business sector, disaster, system, or software. Therefore, only interventions with results that can be extrapolated to organizations with ICT-based processes were included.

The context was retrieved during the data extraction phase of the protocol. Based on these criteria, the authors eliminated publications by abstract, and, in doubt, the full text was read to decide. The research team (student and three supervisors) met, at least, monthly for a progress report and to resolve discrepancies, although frequently maintaining contact when some particular issue arises.

Consequently, the exclusion criteria reduced the set of eligible publications. This was achieved mainly by publications addressing areas not related to the research question, namely post-disaster recovery, building reconstruction, community issues, or psychological effects. Publications considering a specific market sector are also highly reported and excluded when the results did not glimpse the applicability to other organizations. Communications on the events of a specific disaster are also returned. They are excluded when the conclusions referred only to how the organization

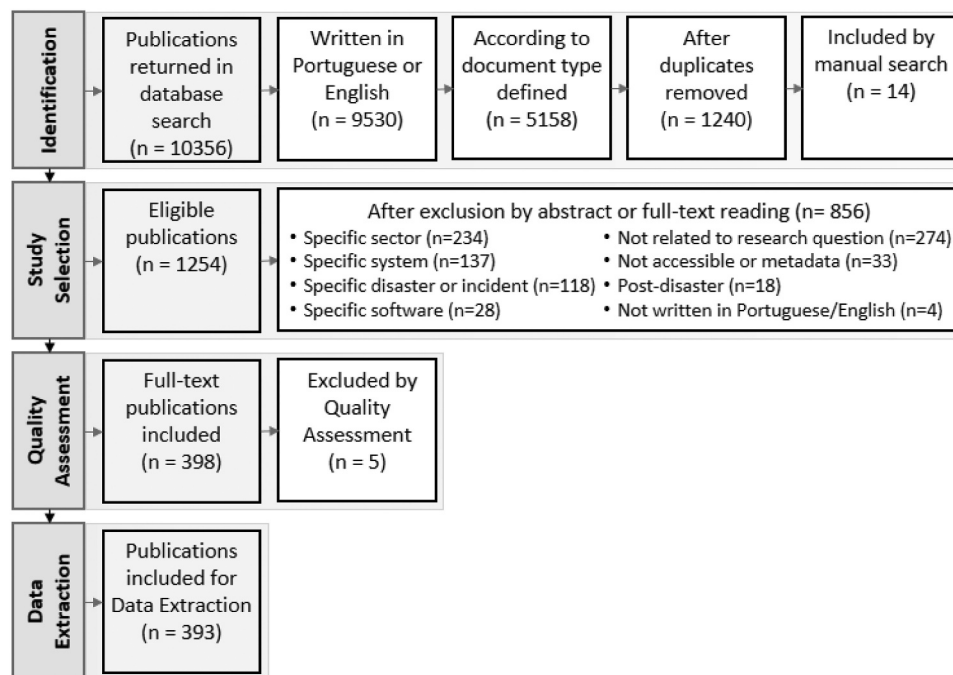


Figure 5. Phases of the implemented protocol following the selection criteria.

coped with the events or were highly adherent to the context of the study. A high number of excluded publications addressed systems or software configurations to enhance business continuity. Examples are: backup & restore procedures, firewall or cloud computing systems configurations, or other highly technical or marked-in-time considerations that do not guarantee medium-term usage.

All full-text publications were read and analyzed for quality assessment to provide still more detailed exclusion criteria (Russo et al., 2021). The objective was to weigh the importance of individual studies for the synthesis, guide the interpretation of findings and determine the strength of the inferences (Kitchenham, 2004). There is a set of six quality questions to assess the study design, presented in Figure 6.

The results are weighted using quality scores, and the study is excluded when the score is less than 2.5 points out of 6.0. If the study answers the quality question, the score is one point, half-point for a partial answer, and no points if not answered. With this process, the 393 publications accepted for Data Extraction are guaranteed to be not duplicated. They are accurately communicating relative

to the research question, with a relevant level of study quality to minimize bias and maximize validity (Kitchenham, 2004).

Aiming to support the literature review findings and reporting, the Data Extraction contained nine questions. The questions presented in Figure 7 are related to the BCM components in which the publication contributes with strategic guidelines.

The Data Extraction questions presented in Figure 7 must be interpreted within the BC context. One focal question is if a publication establishes a measurement process or system for the BCP implementation or design. Another relevant question intends to clarify if the study considers ICT-supported business processes.

#### 4.1. Overall summary

Initially, about 10% of the 1254 articles were eligible, referring to strategic guidelines that apply to all organizations. The other publications (90%) had specific considerations for a population or context, and therefore not included in the quality assessment. The

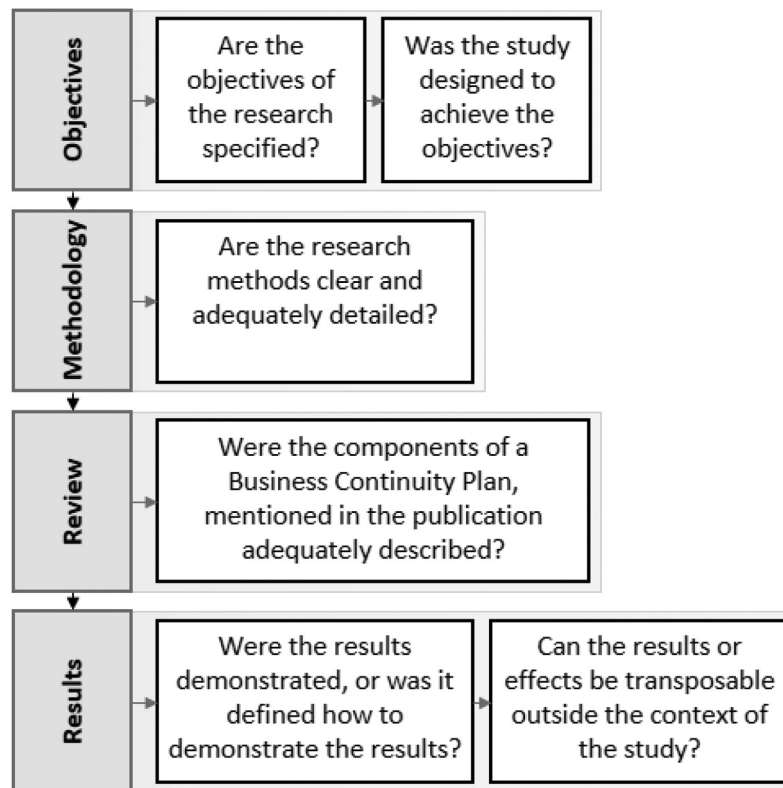
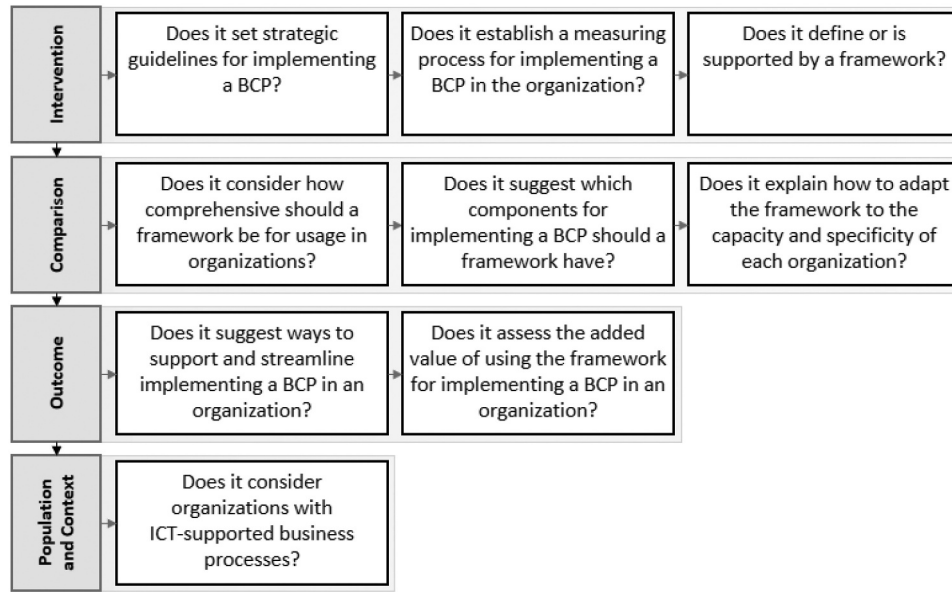


Figure 6. Quality questions of the implemented protocol.





**Figure 7.** Data Extraction questions.

reviewers met to clarify the criteria for excluding publications and included publications that had specific guidelines for the target population or context but could be extrapolated to other organizations. Across the remaining 393 publications, 288 publications focus on comprehensive BC strategic guidelines to apply to all organizations. The other 105 are focusing on BCM components or activities guidelines. Altogether, can be combined or integrated into a comprehensive set of guidelines to streamline the organizational processes for the BCP design.

From the final set of quality-assessed publications, different areas of research were identified, communicating strategic guidelines for specific BCM components or activities. Some publications are addressing, not the isolated BCM component, but the research about a certain disaster, and how can the BCP be designed or updated to include its guidance. Natural disasters and pandemic issues are the main research subjects when not communicating conceptual studies, BC frameworks, or considerations about the preparedness or performance within a BCM component.

#### 4.2. BCM components identified

After the Data Extraction phase, the results highlighted some research focus clusters, along with

various types of populations (e.g. health, oil, banking, or financial organizations). These publications contribute with quality-assessed communications for the outcome, as presented in Figure 8. The clusters of research areas are included in Figure 8, which have an identical structural representation of BCM components, as revealed in Figure 1. In Figure 8, two major research areas have been added: Emergency Response and Crisis Management. Likewise, considerations about Mass Trauma, such as pandemics or outbreaks of infectious disease, influence business processes and arrangements to deal with the events triggered by them. These considerations should be included in the BCP design, such as the preparation of telework resources with ICT support.

The wide area of research on Natural Disasters is also represented in the eligible publications. It is recognized that Natural Disasters comprehend the greatest number of sources of business disruptions. Therefore, the BCP must face the effects of events arising from natural disasters. The BCP should document alternative arrangements for business continuity, e.g., specific strategies in regions often affected by natural disasters or telecommuting. Technical failures, such as hardware or software malfunctions, or Human Threats, such as terrorism, also cause business disruption, reported in the studies as the trigger for actions and planning. Thus, the design of the BCP must consider the

support provided in the strategic guidelines suggested by the studies.

The identified research areas are related to the BCM components shown in Figure 1. Despite the importance for the design of the BCP framework, there were no primary studies with BC Teams as a research purpose. Although, the constitution of BC Teams is mentioned in 19 publications covering the BCM program. Considerations about managing the BCM program are mentioned in 42 publications and 11 publications elaborate on conducting a BCM component as a project.

The shapes added to the BCM components represented in Figure 8 show a trend justified by a greater number of publications on that subject. For example, of the 29 publications about the Administration Support component, 17 publications are addressing the commitment to managing the program or project. Understanding the Organization has valuable insights, represented by 17 publications on how to raise awareness about BC. Concerning organizational culture in

the BCM program or project, 14 publications recognize the broad impact on all stages of BCP design and implementation and on the Plan-Do-Check-Act activities referred to in the Frameworks.

The Risk Assessment (RA) is an essential step for the design of BCP, evidenced by 39 publications on the topic, of the 167 that address risk issues. 20 publications are presenting strategic issues or guidelines for RA. Highlighting some areas of risk, 25 publications address Information Security issues, with 12 publications focusing on cybersecurity and cyberattacks. Regarding Datacenter and Cloud Computing issues, there are 10 publications with strategic design and implementation issues to improve BCP. The risk of financial loss is a concern in 10 publications. 12 publications specifically communicate risk issues in supply chain continuity. Some considerations in the relationships with Suppliers, Contractors, or Service or Product Providers and Outsourcing are mentioned in 8 publications.

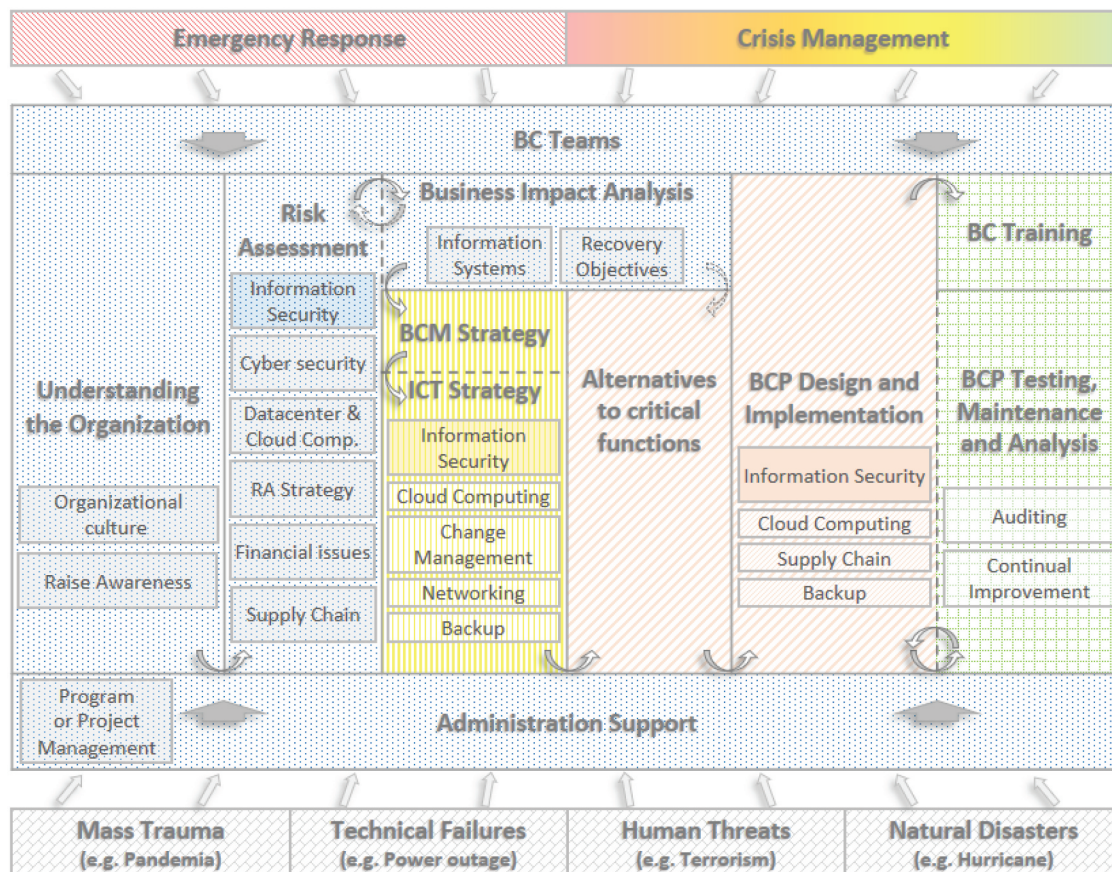


Figure 8. Areas represented in the publications included.

Another relevant step is Business Impact Analysis (BIA), represented by 58 publications. There are 15 publications delivering frameworks, or methodologies, to address BIA or BIA integrated with RA and BCP. IS and ICT are represented by 8 publications, 5 publications address information and data concerns, and 6 publications give relevancy to recovery objectives. There are 11 publications considering strategies for natural disaster impact analysis.

The ICT Strategy area, embedded in the BCM Strategy, an area closer to the research question, totals 129 publications, although with 33 publications that assertively communicate the ICT Strategy guidelines. 23 publications are addressing Information Security issues and 11 publications with specific planning strategic guidelines for dealing with cybersecurity incidents. However, guidelines for improving Datacenter arrangements are also communicated and represented in 30 publications. Of this total, 11 publications have as their subject Cloud Computing and 3 publications elaborate on Virtualization issues. Backup & Restore concerns are discussed in 7 publications with 5 publications addressing Networking issues. IS-specific guidelines are represented in 3 publications. The Change Management topic has 5 publications communicating the implementation of change requests for the ICT infrastructure.

Considering that the search string always includes “business continuity plan” or “disaster recovery plan,” all eligible publications address this topic. Nevertheless, 163 publications have those keywords in the title, therefore directly addressing the strategic guidelines for their design or implementation. Thus, 35 publications proposed frameworks, models, methodologies, or approaches to assertively design a BCP. 31 publications mention Natural Disasters, and 23 publications address Information Security. [Table 1](#) summarizes the number of quality-assessed publications included in the research, considering the activities, issues, or concerns in each of the BCM Components identified in [Figure 8](#).

The quantification shown in [Table 1](#) highlights the number of publications addressing ICT strategic guidance, strengthening the concept of DRP associated with ICT issues. All areas are essential to be considered in designing a BCP, nevertheless,

**Table 1.** Quantitative synthesis of publications, by BCM Component.

BCM Component	Number of publications
Administration Support	29
BC Teams	19
Understanding the Organization	31
Risk Assessment	167
Business Impact Analysis	58
BCM Strategy	121
ICT Strategy	129
Alternatives to critical functions	26
BCP Design and Implementation	163
BC Training	20
BCP Testing, Maintenance, and Analysis	68

some areas will be detailed, because of the relation to the research question context. Aiming to emphasize the Outcome and Context, the areas: ICT Strategy, RA, BIA, and BCP are described in some detail.

### 4.3. Risk assessment

The RA step is important to explore and recognize the threats to BC and the probability of occurrence. Environmental uncertainty, natural disasters, and ICT issues are the primary concerns addressed, and with contributions from the literature. Some authors propose a framework to improve the RA, with a greater focus on BCP that ends with the normal restoration of business, although there are contributions to post-crisis BCP. Justification for the BCM program is one area addressed, using the RA as a starting point to mitigate financial losses and to transfer risk. This is one reason for the supply chain guidelines to be represented in the quality-assessed publications. Other reasons are the geographical dispersion or geo-clustering of the supply chain and lean production. This unrest is followed by issues with providers, contractors, vendors, and, ultimately, outsourcing labor or business processes.

Information Security attacks, events, and mitigation are recurrent topics in RA. Identification of information sources, information flows and inventory or asset management is a trend in this topic. Nevertheless, models or frameworks for RA are proposed, either to capture the risk perception or to support the BIA step. The RA studies also focus on Datacenter and their infrastructures and server virtualization, identifying the risks to be addressed in the BCP or DRP. In this context, studies on



Cloud Computing or cloud-based datacenters are focused on risk prevention of data loss, achievable by the eventual geographical dispersion of data or by replication and redundancy techniques.

#### 4.4. Business impact analysis

The analysis of the impact on business is a research area that spans various topics. In the quality-assessed publications, there are three that stand out: BIA frameworks, BIA considering Information and IS, and the BIA considerations regarding Natural Disasters. BIA frameworks are reported as a key step for BCM, especially for aligning BIA with BCM, but also for understanding business attributes and delivering essential information about the impact of disruptions on business. Considering IS, BIA is reported as the foundation to build DRP strategy, using an inventory of applications and systems to decide inclusion. It is also mentioned that is especially important to establish recovery strategies, having as key components, the Recovery Time Objective (RTO) and Recovery Point Objective (RPO). Some studies address strategies to cope with natural disaster risks, claiming that the BCP must not be developed to consider a specific natural disaster. They propose reviewing the vulnerabilities in business processes, that can be exploited by different natural disasters or other kinds of disruptive events. Mainly to the wide scope of BIA, specific topics and strategies are limited in the publications.

#### 4.5. ICT strategy

The ICT Strategy is relevant to defining the BCP design. It must primarily consider the alternatives to critical functions and the functions that the organization wants to keep delivering, even if they are not critical for its survivability, since they were identified in BIA.

Mainly, ICT Strategy approaches recovery strategies such as backups, alternate computing sites, off-site storage, and transition to cloud computing. The approaches consider information security enhancement and other arrangements or procedures to mitigate the risk of data loss, information unavailability, computation capability, or systems control.

Regarding Cloud Computing, it is represented as a strategy for BC rather than building secondary backup sites. Sometimes, Disaster Recovery as a Service is discussed as a new practice. Some studies introduced Cloud Computing as a solution in combination with Virtualization to sustain operations with minimum cost.

Cybersecurity and cyber-attack mitigation are the primary subjects in the Security area. Challenges in this area include a lack of security culture, expertise in information security and cybersecurity, and the development of security policies. Recover data upon a security incident is a represented concern. A Security Management Program is proposed as a strategic guideline to decrease the probability of incident occurrence.

The recent pandemic events force the adjustment of fundamental aspects of life, foster innovation, and unlock opportunities. Consequentially the impact of remote working on modern ICT architecture leads to important transformations. Modern ICT architectures are key success factors for each and any digital transformation journey, enabling it to evolve iteratively, manage change holistically, and stimulate innovation (Rimboiu, 2020).

Yet, an ICT Architecture plan is required to build success in a digital economy (CompTIA, 2017). One key point of the planning includes architectural planning tightly coupled with digital transformation, not adding just technology but also building new structures and processes. Long-term planning is a new exercise for most organizations in the ability to prioritize investments in different areas, such as the adoption of the Internet of Things (IoT). The plan and the business objectives should be defined first rather than just acquiring technology. Adoption of cloud computing typically involves Software as a Service (SaaS) or migration of an existing system into cloud infrastructure, using strategies like transformation into a cloud-first operation.

#### 4.6. Business continuity plan

The BCP or DRP is mentioned in every one of the quality-assessed publications since they are part of the search string. Nevertheless, some



publications discuss the usefulness of a BCP and propose frameworks. They emphasize the phases identified in Figure 1, e.g., organizational awareness or BCP Training and, especially, the preparatory steps to the design and implementation of a BCP. Previously, we highlighted the number of publications that address security issues focused on cybersecurity and the necessary procedures to mitigate the risk. They define security policies, encourage the security culture, and suggest better preparing ICT professionals with training and practice.

The Natural Disaster topic is mentioned in the publications although normally considering them as an origin for disruptions in business processes. There are few strategic guidelines for addressing specific natural disasters and considering them in the BCP. This can be justified since the BCP should be designed to respond to the impact on business and not designed specifically for a type of disaster. Some publications reveal concerns with supply chain disruptions and present guidelines to cope with those disruptions, discussing that an organization's supply chain BCP must extend to all supply chain participants. Other publications address post-crisis BCP, presenting what organizations should do once a crisis has occurred.

#### 4.7. Research limitations

The SLR considered peer-reviewed published articles, including also books, dissertations, and thesis. When conducting the SLR, during the execution

phase, some constraints occur because of database search engine capabilities. Each search engine deals with the search string differently. One restricts the number of logical operators or the use of wildcards. Another integrates the curator's keywords to refine the focal point of the indexed article or includes the first 1500 words in the search when the abstract is missing (EBSCOConnect, 2021). This integration highly unbalances the number of records returned from EBCSCO, compared with the others. The book document type is not typically designed as a research study, however, it was included in the SLR, always considering a high level of quality, inferred by the author's curriculum. Primary studies are often poorly reported (Kitchenham, 2004), and in a few studies, the assessment was limited when using the quality criterion.

## 5. Findings and discussion

This research aimed to collect primary studies that harvest the guidelines, according to the interventional studies returned. Tables 2–5 presents a synthesis of the highest quality-accessed publications, considering the publication date after 2015 and a quality score higher than 4 points. Before this date, there is a set of publications that report pre-eminent positions of literature related to this research (Herbane, 2010; Maurer & Lechner, 2014; Niemimaa, 2015).

In Table 2, there is a representation of studies by the most found type of studies.

Table 2 shows that the design of models, methodologies, approaches, or frameworks represents

**Table 2.** Quantitative synthesis of findings by most found type of study.

Topic	# of publications	Main references	Contribution
Models, methodologies, approaches, or frameworks	75	(Torabi et al., 2016)- (Segovia, 2017)- (Schätter et al., 2019)- (Sambo & Bankole, 2016)- (Rezaei Soufi et al., 2019)- (Brás & Ribeiro, 2016; Motevali Haghighi & Torabi, 2020)- (Anir et al., 2019)- (Zeng & Zio, 2017)- (Tracey et al., 2017)- (Revilla & Saenz, 2017)- (Somasekaram, 2017)	Focus on improvement of preparedness through a BCM component.
Case studies	62	(Torabi et al., 2016)- (Segovia, 2017)- (Schätter et al., 2019)- (Sambo & Bankole, 2016)- (Sahebjamnia et al., 2018)- (Rezaei Soufi et al., 2019)- (Miranda & Swanstrom, 2020)- (Brás & Guerreiro, 2016)- (Motevali Haghighi & Torabi, 2020)	Presents what was changed to better cope with the disruption within the scope of an organization.
Case studies to validate a framework	19	(Torabi et al., 2016)- (Segovia, 2017)- (Schätter et al., 2019)- (Sambo & Bankole, 2016)- (Rezaei Soufi et al., 2019)- (Motevali Haghighi & Torabi, 2020)- (Somasekaram, 2017)	The case study methodology is often used to validate the proposed artifacts.
Researchers' experience in dealing with disasters	28	(Moore, 2016)- (Burtles, 2016)- (Hatton et al., 2016)	Specific disaster issues are a tendency of the studies returned, especially in the following years after a high dimension disaster.

19% of the extracted studies of the SLR. The report of the professional experience of authors in dealing with disasters is nearly 7% of the extracted studies. Considering studies supported by a case study methodology, the number reaches 15%, and from this set, one-third uses a case study to validate a framework.

Table 3 is a representation of the subjects addressed by the 75 frameworks mentioned in Table 2. The column “# of publications” represents how many studies have a topic area, and one study can address one or more topics represented.

The SCM is a relevant topic that increased the number of publications in the last ten years, representing almost 13% of the extracted studies of the SLR. Nevertheless, frameworks for addressing the common issues of BC still represent 16% of the SLR extracted studies.

The dynamic changes in the environment or the context can generate the need to address the related risk and influence the ICT capabilities. Sometimes the risk is treated by employing new technologies. Therefore, it can require novel approaches in analyses and assessments for effective BCM or be generic to incorporate them. Six publications from 2015 and beyond mention ICT adaptation to changes and research on how BCM can be improved to adapt to changes (Aziz & Jambari, 2019; Brás & Guerreiro, 2016; Labus et al., 2020; Mohammadian & Yamin, 2017; Schätter et al., 2019; Sheffi, 2015).

Table 4 shows studies that report in the methodology or literature review on the use of International Frameworks. This information is relevant to understanding trends in the selection of Frameworks, used in publications.

**Table 3.** Quantitative synthesis of findings by the framework’s subject.

Topic	# of publications	Main references	Contribution
Framework addressing the BCM program	23	(Torabi et al., 2016)- (Segovia, 2017)- (Schätter et al., 2019)- (Motevali Haghighi & Torabi, 2020)- (Anir et al., 2019)- (Zeng & Zio, 2017)	Focus on improvement of program management or performance.
BCP frameworks	21	(Sambo & Bankole, 2016)- (Rezaei Soufi et al., 2019)- (Brás & Ribeiro, 2016)- (Tracey et al., 2017)	Focus on the steps for achieving a comprehensive BCP.
DRP frameworks	8	(Brás & Ribeiro, 2016)- (Somasekaram, 2017)	These works consider cloud computing and systems transition decision-making.
Risk Management frameworks	12	(Torabi et al., 2016)- (Revilla & Saenz, 2017)	Some of the works approach statistical studies or mathematical equations to demonstrate the framework’s effectiveness.
Frameworks addressing BC Teams’ issues	0		BC Teams’ issues are not the primary focus of BC frameworks research.
Frameworks considering the Supply Chain	30	(Montshiwa et al., 2016)	Relevancy and issues of Supply Chain Management (SCM) in case of disruption.
Frameworks formally managing the Supply Chain	12	(Schätter et al., 2019)- (Revilla & Saenz, 2017)	
Referencing a Framework to support SCM	8	(Suresh et al., 2020)- (Hopkin, 2017)	The main focus is Risk Management. 6 of these works provide a new framework for SCM.
Referencing a Framework to cope with new threats	18	(Schätter et al., 2019)- (Russo & Reis, 2020c)- (Gordon & Salazar-Chacon, 2020)- (Calder, 2020)- (Tripathi & Bagga, 2020)- (AlHamdani, 2020)- (Bajgorić et al., 2020)- (Phillips & Landahl, 2021)	These works consider Mass Trauma (e.g. COVID-19 pandemic), Human Threats (e.g. Terrorism), and other emerging threats and challenges related to ICT.

**Table 4.** Quantitative synthesis of findings by Framework used in the study.

Topic	# of publications	Main references	Contribution
Adoption of a BCM Framework	<b>37</b>		Proposes an artifact to streamline processes or procedures to business process continuity. Some publications mention more than one Framework in their literature review section.
Referencing ISO 22301	L 17	(Păunescu, 2017)	
Referencing ITIL	L 11	(Putra & Nazief, 2018)	
Referencing COBIT	L 8	(Iqbal et al., 2016)	
Referencing CMMI	L 1	<2016	
Referencing ISO 27001	6	(Gordon & Salazar-Chacon, 2020)	These works consider the protection of information security in case of disruption or incident.

**Table 5.** Quantitative synthesis of findings by measurement related topics.

Topic	# of publications	Main references	Contribution
Addressing measurement issues	38		These works from 2000 and forward consider measurement for specific issues, not for the entire BCM program.
Mentioning measurement	└ 14	(Vaidyanathan, 2017)- (Ricks & Boswell, 2019)- (Bajgorić et al., 2020)	These works do not propose specific Key Performance Indicators (KPI) or metrics, mainly suggesting the usage of RTO and RPO and RA measurement.
Mention or propose KPI or metrics for different reasons	└ 24		From 2018 and forward, 3 publications mention metrics, KPI, or measurement concepts.
Metrics or KPI for ICT systems	└ 10	(Iqbal et al., 2016)- (Ream & Mathew, 2018)- (Gardner, 2016)	These works are focused on the understanding of an organization's preparedness and readiness. One publication is from 2018 and forward.
RTO and RPO	└ 2	<2016	These works focus on metrics for DRP performance assessment.
ICT system metrics in BCM or BCP	└ 3	(Iqbal et al., 2016)- (Ream & Mathew, 2018)	These works focus on engaging metrics for BCM program justification or BCP readiness.
Metrics in RA	└ 7	(Zeng & Zio, 2017)	These works are focused on loss prevention or BCM program or project justification. Some works propose a risk index based on metrics.
Metrics or KPI for BCM or BCP	└ 7	(Zeng & Zio, 2017)	Some works propose metrics for BCM or BCP justification, readiness, or financial loss, focusing on keeping executive support and engagement.

From the SLR extracted studies, 43 adopted an International Framework in their research, not proposing a new one. Table 4 evidentiates the adoption of the ISO 22301 framework as the primary Framework for BC. The ISO 27001 provides requirements for an Information Security Management System, a relevant subarea of BC. Cybersecurity and Datacenter issues are common topics in these studies.

In Table 5, the number of publications, that address measurement issues, represents nearly 10% of the extracted SLR studies. This percentage confirms the relevancy of BC measurement.

The information contained in Table 5 reveals that 6% of the SLR extracted studies mention or propose KPI or metrics for different reasons, namely for ICT systems or RA. Most of the 2% of extracted studies, addressing metrics or KPI for BCM or BCP, is focused on financial justification or loss, aiming to keep executive support and engagement.

All the extracted studies in the SLR contribute to the clarification of the research question. Most of the studies, presented in Tables 2 to 5, concluded their study applies to the target population, although generalizable for most organizations. There is a wide set of studies that communicate how to support the organizational process to achieve a higher BC capacity. Hence, some conclusions can be outlined from this review to provide directions for future research, for example, exploring risk management by considering cloud computing or transitioning to the cloud. Nevertheless, there is a gap in the recent literature related to

metrics design applicable to relevant BCM components and activities to achieve a BCP. Some books provide a set of good practices for a comprehensive approach to BCM, but also with gaps in metrics design that can provide an answer to the research question.

A key principle in management is Controlling, or the process of evaluating and regulating ongoing activities to ensure that goals are achieved (Pride et al., 2013). According to the Project Management Institute (PMI, 2017), the Monitor and Control Project Work is the process of tracking, reviewing, and reporting the overall progress to meet the performance objectives defined in the project management plan. One contribution of this SLR is to collect studies that can provide benchmarking and performance standards for achieving some benefits. One of the benefits is to allow stakeholders to understand the project's current state and have visibility into the future project status (PMI, 2017). To do this, researchers must capture all strategic guidelines in the intervention from the resulting quality-assessed studies. Essentially, all the success factors, guidelines, or good practices can be used to benchmark and streamline the BCP design, carefully supported by a set of metrics with defined goals. By addressing these issues and incorporating them into the proposed framework, the organizational processes can be effectively supported, streamlining the implementation of a BCP according to the maturity and capacity of the organization.

The descriptive analysis of this study provides evidence related to the identification of gaps in the formal definition of metrics in the Frameworks identified in [Figure 2](#). The key evidence returned is the gap in studies reporting the design of metrics to identify what needs to be measured to evaluate the organizational BC maturity. The Frameworks mentioned in this work were updated after 2018, and there is a gap in new research using these recent versions.

## 6. Conclusion

This study has established that there are many communications related to business continuity planning, especially obtained from natural disaster communications. It strengthens the proposition that business continuity issues and constraints will always affect organizations, their people, processes, and technology.

The major contribution of this study is to provide an SLR, using the EBSE protocol, that positions the research activity (Kitchenham, 2004). This SLR supports the research by revealing where are, in the publications, the good practices, success factors, or strategic guidelines for the design of a BCP. The SLR value-added is the identification and quantification of BC studied areas that are communicated and where there are potential gaps. The detailed quantification of studies allows us to understand if researchers are communicating their applied experience, validating their reported guidelines. The quantification of Frameworks is useful to validate the selection of Frameworks in the gap analysis of the study.

The analysis of the 393 publications resulted in several main ideas:

- Overview of the most adopted Frameworks across several organizations referred to in the publications to adjust the proposed framework to its considerations;
- Identification and overview of the BCM components and activities considering the challenges of modern ICT;
- A comprehensive summary of best practices and guidelines for BCM Program measurement and its components and activities;
- Raise awareness on underestimated areas to tackle and cope with, like Supply Chain Management, Change Management, or BC Teams;
- A research path that includes the COVID-19 pandemic and post-pandemic issues, but also for emerging technology treats and challenges, like OT-IT-CT integration in terms of architecture design.

This review highlights that there are still gaps, identified in [Figure 2](#), in the degree to which the authors and Frameworks are communicating what needs to be measured and the key metrics on each BCM component or activity. Measurement allows perceiving the level of fulfillment compared to a desirable function for the BCM activity. The creation of metrics and interpretation of its results can point out what areas there is the need to take action to be prepared for business function disruptions, or incidents. Project success is measured at the end of the project, whereas performance measurement is over the project-life cycle (Müller, 2019). The performance measurement baselines in the Monitoring and Controlling Process Group can be enhanced by providing specific information about work performance information or data, for validating or controlling scope, quality, resources, or monitoring risks or stakeholder engagement (PMI, 2017). Considering that few primary studies are addressing what needs to be measured, there are gaps in understanding what metrics can assess the capacity or maturity in the BCM activities' achievement.

Furthermore, there are a set of interventions that aim to improve outcomes related to understanding the BCM component or activity. Nevertheless, only a few communicating metrics and fewer are not focused on justifying the investment in the BCM program, RA, ICT systems metrics, RTO and RPO kind of metrics. Post-disaster metrics are also a future research area to evaluate the organization's response after the disaster and the crisis.

However, the SLR made it possible to identify and relate the BCM components. It also allowed identifying where are the guidelines to be considered for the design of the proposed framework. The framework aims to narrow the identified gaps, allowing organizations to assess



BCM performance and organizational maturity that guarantee a specified level of preparedness. With this in consideration, this review substantiates the foundations for the research in progress. It points to future research: types of metrics, standards or thresholds, and parameters for evaluating BC performance and preparedness of an organization.

## Disclosure statement

No potential conflict of interest was reported by the author(s).

## ORCID

Nelson Russo  <http://orcid.org/0000-0001-9664-7148>  
 Leonilde Reis  <http://orcid.org/0000-0002-4398-8384>  
 Clara Silveira  <http://orcid.org/0000-0003-2809-4208>  
 Henrique S. Mamede  <http://orcid.org/0000-0002-5383-9884>

## References

- AlHamdani, W. A. (2020). Resilient cybersecurity architecture. *Proceedings of the International Conference on Cyber Warfare & Security*, Islamabad, Pakistan, (pp. 23–32). <https://doi.org/10.34190/ICCWS.20.011>
- Anir, H., Fredj, M., & Kassou, M. (2019). Towards an approach for integrating business continuity management into enterprise architecture. *International Journal of Computer Science & Information Technology (IJCSIT)*, 11 (02), 11. <https://doi.org/10.5121/ijcsit.2019.11201>
- Aziz, N. M., & Jambari, D. I. (2019). Information management procedures for business continuity plan maintenance. 2019 *International Conference on Electrical Engineering and Informatics (ICEEI)*, (pp. 489–495). Bandung, Indonesia. <https://doi.org/10.1109/ICEEI47359.2019.8988804>
- Bajgorić, N., Turulja, L., Ibrahimović, S., & Alagić, A. (2020). *Enhancing business continuity and IT capability: system administration and server operating platforms*. CRC Press.
- Brás, J., & Guerreiro, S. (2016). Designing Business Continuity Processes Using DEMO: An Insurance Company Case Study. In R. Pergl, M. Molhanec, E. Babkin, S. Fosso Wamba (Eds.), *Enterprise and Organizational Modeling and Simulation. EOMAS 2016. Lecture Notes in Business Information Processing* (Vol. 272, pp. 154–171). Springer, Cham. [https://doi.org/10.1007/978-3-319-49454-8\\_11](https://doi.org/10.1007/978-3-319-49454-8_11)
- Brás, J., & Ribeiro, R. (2016). Business Continuity and Disaster Recovery: An Overview, Trends and Challenges. 13th *International Conference on Information Systems & Technology Management-CONTECSI*, São Paulo, Brazil, (pp. 1698–1719). <https://doi.org/10.5748/9788599693124-13CONTECSI/PS-3893>
- Brereton, P., Kitchenham, B. A., Budgen, D., Turner, M., & Khalil, M. (2007). Lessons from applying the systematic literature review process within the software engineering domain. *The Journal of Systems and Software*, 80(4), 571–583. <https://doi.org/10.1016/j.jss.2006.07.009>
- Burtles, J. (2016). *Manager's guide to business continuity exercises: Testing your plan*. Rothstein Publishing eBook Collection.
- Calder, A. (2020). *ISO 22301: 2019 - an introduction to a business continuity management system (BCMS)*. ITGP. <https://doi.org/10.2307/j.ctv131bwtk>
- Cerullo, V., & Cerullo, M. J. (2004). Business continuity planning: A comprehensive approach. *Journal Information Systems Management*, 21(3), 70–78. <https://doi.org/10.1201/1078/44432.21.3.20040601/82480.11>
- CMMI Institute. (2018). *CMMI Model V2.0*. Pittsburgh, PA: CMMI Institute.
- CompTIA. (2017). *Planning A Modern It Architecture*. Retrieved from <https://connect.comptia.org/content/research/planning-a-modern-it-architecture>
- Cook, D. J., Mulrow, C. D., & Haynes, R. B. (1997). Systematic reviews: synthesis of best evidence for clinical decisions. *Academia and Clinic*, 126(5), 376–380. <https://doi.org/10.7326/0003-4819-126-5-199703010-00006>
- EBSCOConnect. (2021). *Hello-How can we help?* Retrieved January 22, 2021, from [https://connect.ebsco.com/s/?language=en\\_US](https://connect.ebsco.com/s/?language=en_US)
- Fani, S. V., & Subriadi, A. P. (2019). Business continuity plan: Examining of multi-usable framework. *Procedia computer science*, 275–282. <https://doi.org/10.1016/j.procs.2019.11.124>
- Fryt, M. (2019). Process Maturity Models - Applicability and Usability Review. *World Scientific News*, 129, 51–71.
- Gardner, B. (2016). *An exploratory qualitative inquiry of key indicators on IT disaster recovery planning* Doctoral dissertation, Capella University.
- Gordon, A., & Salazar-Chacon, G. (2020). DRP Analysis: Service Outage in Data Center due to Power Failures. 11th *Annual IEEE Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Vancouver, BC, Canada, (Vol. 2020, pp. 0182–0187). <https://doi.org/10.1109/IEMCON51383.2020.9284920>
- Haddaway, N. R., & Macura, B. (2018). The role of reporting standards in producing robust literature reviews. *Nature Climate Change*, 8(6), 444–447. <https://doi.org/10.1038/s41558-018-0180-3>
- Hatton, T., Grimshaw, E., Vargo, J., & Seville, E. (2016). Lessons from disaster: Creating a business continuity plan that really works. *Journal of Business Continuity & Emergency Planning*, 10(1), 84–92.
- Herbane, B. (2010). The evolution of business continuity management: A historical review of practices and drivers. *Business History*, 52(6), 978–1002. <https://doi.org/10.1080/00076791.2010.511185>
- Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *Management Information Systems Quarterly*, 28(1), 75–105. <https://doi.org/10.2307/25148625>

- Hibberd, G. (2011). Developing a BCM Strategy in Line with Business Strategy. In A. Hiles (Ed.), *The Definitive Handbook of Business Continuity Management* (3rd ed., pp. 23–30). Nova Jersey, USA: John Wiley & Sons.
- Hopkin, P. (2017). *Fundamentals of risk management: understanding, evaluating and implementing effective risk management*. (4th ed.). Kogan Page.
- Iqbal, A., Widyawan A., & Mustika, I. W. (2016). COBIT 5 domain delivery, service and support mapping for business continuity plan. *AIP Conference Proceedings*, Yogyakarta, Indonesia, (Vol. 1746, pp.1–6). <https://doi.org/10.1063/1.4953970>
- ISACA. (2018). *COBIT 2019 framework - governance and management objectives*.
- Isa, M., Fauzi, A., & Susilowati, I. (2019). Flood risk reduction in the northern coast of central Java Province, Indonesia: An application of stakeholder's analysis. *Jamba: Journal of Disaster Risk Studies*, 11(1). <https://doi.org/10.4102/jamba.v11i1.660>
- ISO 22301. (2019). *Societal security - Business continuity management systems - Requirements*. Switzerland: ISO.
- ISO 22316.(2017). *Security and resilience - Organizational resilience - Principles and attributes*. Switzerland: ISO.
- ISO/IEC 22989. (2022). *Information technology - Artificial intelligence - Artificial intelligence concepts and terminology*.
- ISO/IEC 27005. (2018). *Information technology - Security techniques - Information security risk management*. ISO/IEC.
- ISO/IEC 29180. (2012). *Information technology - Telecommunications and information exchange between systems - Security framework for ubiquitous sensor networks*. ISO/IEC.
- ISO/IEC TS 22237-30. (2022). *Information technology - Data centre facilities and infrastructures - Part 30: Earthquake risk and impact analysis*. ISO/IEC TS.
- ITIL. (2019). *ITIL Foundation ITIL (4 Edition. ed.)*. AXELOS.
- Kitchenham, B. (2004). *Procedures for performing systematic reviews*. Keele University.
- Kliem, R. L., & Richie, G. D. (2016). *Business continuity planning: A project management approach*. Auerbach Publications.
- Labus, M., Despotović-Zrakić, M., Bogdanović, Z., Barać, D., & Popović, S. (2020). Adaptive E-Business continuity management: Evidence from the financial sector. *Computer Science & Information Systems*, 17(2), 553–580. <https://doi.org/10.2298/CSIS190202037L>
- Mansol, N. H., Mohd Alwi, N. H., & Ismail, W. (2015). Managing organizational culture requirement for business continuity management (BCM) implementation using goal-question-metric (GQM) approach. *2015 IEEE Conference on Open Systems (ICOS)*, Melaka, Malaysia, (pp. 85–90). <https://doi.org/10.1109/ICOS.2015.7377283>
- Maurer, F., & Lechner, U. (2014). From Disaster Response Planning to e-Resilience: A Literature Review. *BLED 2014 Proceedings*, Bled, Slovenia, (Vol. 32, pp. 1–19). <https://aisel.aisnet.org/bled2014/32>
- Miranda, V. E., & Swanstrom, M. (2020). Surviving disasters: A multi-company case study on disaster recovery plans. *Journal of Applied Business & Economics*, 22(6), 87–105.
- Mohammadian, M., & Yamin, M. (2017). Intelligent decision making and analysis using fuzzy cognitive maps for disaster recovery planning. *International Journal of Information Technology*, 9(3), 225–238. <https://doi.org/10.1007/s41870-017-0027-6>
- Moher, D., Shamseer, L., Clarke, M., Ghersi, D., Liberati, A., Petticrew, M., Stewart, L., Stewart, L. (2015). Preferred Reporting Items for Systematic Review and Meta-Analysis Protocols (PRISMA-P) 2015 statement. *Systematic Reviews*, 4(1), 1–9. <https://doi.org/10.1186/2046-4053-4-1>
- Montshiwa, A. L., Nagahira, A., & Ishida, S. (2016). Modifying business continuity plan (BCP) towards an effective auto-mobile business continuity management (BCM): A quantitative approach. *Journal of Disaster Research*, 11 (4), 691–698. <https://doi.org/10.20965/jdr.2016.p0691>
- Moore, G. D. (2016). *IT disaster response: Lessons learned in the field*. Apress.
- Motevali Haghighi, S., & Torabi, S. (2020). Business continuity-inspired fuzzy risk assessment framework for hospital information systems. *Enterprise Information Systems*, 14(7), 1027–1060. <https://doi.org/10.1080/17517575.2019.1686657>
- Müller, R. (2019). Governance, governmentality and project performance: The role of sovereignty. *International Journal of Information Systems and Project Management*, 7(2), 5–17. <https://doi.org/10.12821/ijispm070201>
- NFPA 1600. (2019). *NFPA 1600® Standard on Continuity, Emergency, and Crisis Management*. National Fire Protection Association.
- 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, 69–105. <https://doi.org/10.17705/1CAIS.03704>
- Păunescu, C. (2017). How prepared are small and medium sized companies for business continuity management? *Quality - Access to Success*, 18(161), 43–48.
- Pereira, J., Varajão, J., & Takagi, N. (2021). Evaluation of information systems project success – Insights from practitioners. *Information Systems Management*, 39(2), 138–155. <https://doi.org/10.1080/10580530.2021.1887982>
- Phillips, B. D., & Landahl, M. (2021). *Business continuity increasing workplace resilience to disasters*. Elsevier Inc.
- PMI. (2017). *A guide to the project management body of knowledge (PMBOK® Guide) (6th ed.)*. Project Management Institute.
- Pride, W. M., Kapoor, J. R., & Hughes, R. J. (2013). *Business*. Cengage Learning.
- Putra, E. P., & Nazief, B. A. (2018). Analysis of Main Cause Factors and Improvement Recommendation of IT Disaster Recovery Problems: A Case Study of XYZ Organization. *AIP Conference Proceedings*, Surakarta, Indonesia, (Vol.1977, 020024, pp. 1–7). <https://doi.org/10.1063/1.5042880>
- Ramakrishnan, R. K., & Viswanathan, S. (2011). The Importance of Business Strategy in Business Continuity Planning. In A. Hiles (Ed.), *The Definitive Handbook of Business Continuity Management* (3rd ed., pp. 31–36). New Jersey, USA: John Wiley & Sons.

- Ream, S., & Mathew, S. (2018). A metrics framework to get and keep management engaged. *Journal of Business Continuity & Emergency Planning*, 11(4), 298–308.
- Revilla, E., & Saenz, M. J. (2017). The impact of risk management on the frequency of supply chain disruptions. *International Journal of Operations & Production Management*, 37(5), 557–576. <https://doi.org/10.1108/IJOPM-03-2016-0129>
- Rezaei Soufi, H., Torabi, S., & Sahebjamnia, N. (2019). Developing a novel quantitative framework for business continuity planning. *International Journal of Production Research*, 57(3), 779–800. <https://doi.org/10.1080/00207543.2018.1483586>
- Ricks, M., & Boswell, L. (2019). Assessing the resilience of an IT portfolio. *Journal of Business Continuity & Emergency Planning*, 13(1), 22–31.
- Rimboiu, C. (2020). Modern IT architecture to manage change, foster innovation. CXOtoday Corner Office. Retrieved from <https://www.cxotoday.com/corner-office/modern-it-architecture-to-manage-change-foster-innovation/>
- Röglinger, M., Pöppelbuß, J., & Becker, J. (2012). Maturity models in business process management. *Business Process Management Journal*, 18(2), 328–346. <https://doi.org/10.1108/14637151211225225>
- Russo, N., & Reis, L. (2020a). *Programas de Faturação Certificados - Guia Prático para a Continuidade de Negócio*. FCA - Editora de Informática.
- Russo, N., & Reis, L. (2020b). Chapter 10 - Methodological approach to systematization of business continuity in organizations. In L. C. Carvalho, Reis, L., Prata, A., & Pereira, R. *Handbook of research on multidisciplinary approaches to entrepreneurship, innovation, and ICTs* (pp. 200–223). IGI Global. <https://doi.org/10.4018/978-1-7998-4099-2.ch010>
- Russo, N., & Reis, L. (2020c). Updated analysis of business continuity issues underlying the certification of invoicing software, considering a pandemic scenario. *Advances in Science, Technology and Engineering Systems Journal*, 5(6), 845–852. <https://doi.org/10.25046/aj0506101>
- Russo, N., Reis, L., Silveira, C., & Mamede, H. S. (2021). Framework for designing Business Continuity - Multidisciplinary Evaluation of Organizational Position Paper. 16th Iberian Conference on Information Systems and Technologies (CISTI), Chaves, Portugal, (pp. 1–4). <https://doi.org/10.23919/CISTI52073.2021.9476297>
- Sahebjamnia, N., Torabi, S., & Mansouri, S. (2018). Building organizational resilience in the face of multiple disruptions. *International Journal of Production Economics*, 197, 63–83. <https://doi.org/10.1016/j.ijpe.2017.12.009>
- 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 and Computer Engineering (IJECE)*, 6(5), 2425–2431. <https://doi.org/10.11591/ijece.v6i5.11461>
- Schätter, F., Hansen, O., Wiens, M., & Schultmann, F. (2019). A decision support methodology for a disaster-caused business continuity management. *Decision Support Systems*, 118, 10–20. <https://doi.org/10.1016/j.dss.2018.12.006>
- Segovia, F. (2017). *Developing a Framework for Business Continuity Management within Local Government*. (Master Thesis) University of Wollongong.
- Sheffi, Y. (2015). *The power of resilience: How the best companies manage the unexpected*. The MIT Press.
- Somasekaram, P. (2017). *A Component-based Business Continuity and Disaster Recovery Framework Master's Dissertation*. Uppsala University.
- Suresh, N., Sanders, G., & Braunscheidel, M. (2020). Business continuity management for supply chains facing catastrophic events. *IEEE Engineering Management Review, Engineering Management Review*, 48(3), 129–138. <https://doi.org/10.1109/EMR.2020.3005506>
- Torabi, S. A., Giahi, R., & Sahebjamnia, N. (2016). An enhanced risk assessment framework for business continuity management systems. *Safety Science*, 89, 201–218. <https://doi.org/10.1016/j.ssci.2016.06.015>
- Tracey, S., O'sullivan, T., Lane, D., Guy, E., & Courtemanche, J. (2017). Promoting resilience using an asset-based approach to business continuity planning. *SAGE Open*, 7(2). <https://doi.org/10.1177/2158244017706712>
- Tripathi, A., & Bagga, T. (2020). Leveraging work from home for business continuity during COVID-19 pandemic-with reference to Bi solution adoption. *Indian Journal of Economics and Business*, 19(1), 19–34.
- Vaidyanathan, K. (2017). Post-event reviews: Using a quantitative approach for analysing incident response to demonstrate the value of business continuity programmes and increase planning efficiency. *Journal of Business Continuity & Emergency Planning*, 11(2), 107–116.
- Varajão, J., & Amaral, A. (2021). Risk management in information systems projects: It can be risky not to do it. *International Journal of Project Management and Productivity Assessment (IJPMPA)*, 9(1), 58–67. <https://doi.org/10.4018/IJPMPA.20210101.0a>
- Wan, Z., Gao, Z., Renzo, M. D., & Hanzo, L. (2022). The road to industry 4.0 and beyond: A communications-, information-, and operation technology collaboration perspective. *ArXiv*, 36(6), 157–164. <https://doi.org/10.48550/arXiv.2205.04741>
- Wong, W. N. (2009). The strategic skills of business continuity managers: Putting business continuity management into corporate long-term planning. *Journal of Business Continuity & Emergency Planning*, 4(1), 62–68.
- Young, T., Rohwer, A., Volmink, J., & Clarke, M. (2014). What are the effects of teaching evidence-based health care (EBHC)? Overview of systematic reviews. *Plos One*, 9(1), e86706. <https://doi.org/10.1371/journal.pone.0086706>
- Zeng, Z., & Zio, E. (2017). An integrated modeling framework for quantitative business continuity assessment. *Process Safety & Environmental Protection: Transactions of the Institution of Chemical Engineers Part B*, 106, 76–88. <https://doi.org/10.1016/j.psep.2016.12.002>