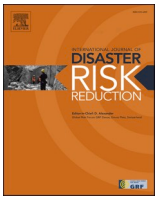
International Journal of Disaster Risk Reduction 124 (2025) 105526

Contents lists available at ScienceDirect

International Journal of Disaster Risk Reduction

journal homepage: www.elsevier.com/locate/ijdrr



Ontological framework for horizon scanning of business continuity of essential services

Oussema Ben Amara [a,b,*], Antonio De Nicola [b], Daouda Kamissoko [a], Frédérick Bénaben [a], Ygal Fijalkow [c]

[a] Industrial Engineering Center, IMT Mines Albi, Albi, France
[b] ENEA - CR Casaccia, Rome, Italy
[c] CERTOP Laboratory, INU Champollion, Albi, France

ARTICLE INFO

Keywords:
Business continuity
Risk management
Systematic literature review
Ontology engineering
Disaster recovery

ABSTRACT

Keeping up essential operations in the face of more complicated disruptions from crises that impact essential services such as healthcare, public transit, and government operations is a major challenge for business continuity (BC) research. Taking up this issue in the midst of increased academic discussion emphasizes how urgent it is to create a thorough reference on BC principles. This paper uses a recently developed BC ontological framework to give a comprehensive review of the literature focused on BC research. The report summarizes a comprehensive investigation of important BC aspects, including technological aspects and the urgent difficulties in maintaining BC sustainability. Through the integration of many viewpoints, this study advances a unified awareness of BC dynamics, promoting a general understanding that is necessary for risk management which is both efficient and lasting for organizations.

1. Introduction

Nowadays, science is confronted with what is perhaps the greatest challenge of all time: a global, multifaceted socio-environmental crisis [1]. Environmental difficulties such as global warming and natural disasters, recently highlighted by the natural sciences, have been compounded by long-standing social, political, and economic challenges extensively studied by the social sciences [1–3]. This convergence of crises presents scenarios ranging from widespread devastation to the potential collapse of industrial civilization [1].

The consequences of these disruptive events—whether fire, flood, pandemics, or terrorist attacks—are increasingly severe. As our society becomes more complex and interconnected, these events occur more frequently, disrupt the environment further, and amplify societal vulnerability [4]. **In this context, the resilience and continuity of Critical Infrastructures (CIs)**—which underpin essential services such as power generation facilities, transportation, healthcare, and finance—are paramount to ensuring societal stability during crises.

To mitigate these risks, organizations implement Business Continuity (BC) strategies. While BC is often assumed to be primarily the concern of businesses, it is particularly relevant for CIs that provide critical services vital to the functioning of society [5,6]. **CIs such as healthcare, transportation, and digital infrastructure are highly vulnerable to disruption, and their protection requires robust BC planning to maintain essential operations during crises.** This paper emphasizes the indispensable role BC plays in

* Corresponding author. IMT Mines Albi, Campus Jarlard, ALBI, CT CEDEX 09 81013, France.
E-mail address: oussema.ben_amara@mines-albi.fr (O. Ben Amara).

https://doi.org/10.1016/j.ijdrr.2025.105526
Received 26 August 2024; Received in revised form 3 April 2025; Accepted 25 April 2025
Available online 3 May 2025

ensuring the resilience of CIs, particularly during disasters that threaten public well-being.

The four phases of crisis management—**preparedness, response, recovery, and mitigation**—highlight the essential role of preparation in Business Continuity Management (BCM), as it involves planning for the uninterrupted operation of essential services [7]. BC focuses on maintaining the functionality of critical business processes during disruptive events, making it a vital component of risk management for both private and public entities, especially those managing CIs [8].

This article provides a novel perspective on the interplay between BC and CIs by examining the unique challenges posed by crises to essential services, such as healthcare, public transportation, and government operations. By developing an ontological framework for horizon scanning, this research explores how BC strategies can be optimized to enhance CI resilience, particularly in the face of increasing socio-environmental crises. This focus offers a more nuanced understanding of BC, emphasizing the specific challenges and resilience measures required to manage CIs effectively.

The primary objectives of this paper are.

(1) To define the scope and environment of BC, particularly its application within CIs, including technology, organization, and human roles;
(2) To explore foundational elements and key examples of BC strategies that safeguard critical services; and
(3) To examine methodologies and applications of BC within CI contexts, emphasizing their importance in mitigating disaster-related risks.

To achieve these objectives, we first provide an overview of BC definitions and adopt the framework most suitable for CIs. We then explain the systematic literature review methodology used to create the ontological framework. Finally, we answer the research questions by querying the ontology and analyzing the results.

The rest of the paper is structured as follows. Section 2 explores BC definitions and outlines the research questions. Section 3 details the development and implementation of the BC ontology, as well as the literature review findings. Section 4 addresses the research questions, providing detailed query results and their interpretations.

2. Defining the business continuity and the research questions

2.1. What is the business continuity?

Business Continuity along with its organizational concepts (BC planning, management, etc.) has several definitions in the literature that are mostly complementary with slight nuances depending on the context (e.g. crisis management, decision making, disaster recovery, Plan-Do-Check-Act cycle, etc) and the application field such as Information Technologies (IT), Supply Chain (SC) and so forth. These definitions should be demarcated before any discussion of the business continuity processes and aspects. In this section, the major distinct definitions resulting from our literature review work (query "business continuity" on Scopus) are presented.

1. "BC is the ability of a business to continue operations during a failure or disaster" [9,10]
2. "BC involves managing contingency measures to ensure critical business processes run during disruptions, covering incident response and disaster recovery" [8].
3. "BC Management is a holistic approach to building resilience, protecting key stakeholders, reputation, and value creation" [11].
4. "BC Planning ensures income continuity during a crisis" [12,13].
5. "BC is delivering products/services at acceptable levels after a disruption" [14,15].
6. "BC uses best practices to mitigate risks and protect stakeholders" [16].
7. "BC planning identifies risks, formulates continuity strategies, and develops reliable continuity plans" [17].

The BC definition adopted by the paper.

This research work considers thus the following definition (combining definitions 1, 3, 5, 6 and 7):

"**BC** is a **holistic management strategy (plan/process in the case of a BCP**) that identifies **potential threats** to an organization, as well as the threats' impacts and that provides a framework to **build the organization's resilience**, with an effective response capability that preserves the interests of its key stakeholders, its reputation, its brand, and its value-producing '*vital*' activities."

To protect the **interests of important stakeholders**, reputation, brand, and value-creating activities, the adopted definition of BC emphasizes BC as a comprehensive management process that **recognizes possible effects**, **fosters resilience**, and **guarantees an efficient response**. Furthermore, it acknowledges BC as **an organization's capacity to carry on providing goods or services after a disruptive event at levels that are acceptable and predetermined**.

2.2. The research questions

Before conducting the research methodology, results and discussions of this paper, the research questions are introduced within this section.

In the general context of "**What steps can we take to enhance our comprehension of BC and its present state-of-the-art, and subsequently evaluate it effectively?**", this paper proposes a **design, implementation and exploitation process of a BC ontological framework** and addresses basically three main research questions which are the following.

RQ1. the first research question of the article is concerned with determining the scope of business continuity (BC). It is trying to figure out **in which areas of technology, environment, organization, and human work roles BC is positioned.**

As BC ensures that an enterprise is able to protect itself against the risks which are inherent in its environment [18], the identification and definition of the elements composing the BC environment is an important step in establishing the BC strategy.

RQ2. the second research question focuses on the underlying theory and principles of Business Continuity (BC) strategies and planning. This includes exploring the fundamental elements of BC and identifying key examples that demonstrate its importance. **What are the essential foundations of Business Continuity and the most noteworthy illustrations of its implementation?**

RQ3. the third research question of this article tackles the applicable aspect of the BC such as its methodologies and applications. **What methodologies have been used for BC? How can we apply them?**

In summary, RQ1 represents the "Environment" part of the framework (technology, environment, organization, and human roles), providing the business needs and ensuring relevance to the research work, while RQ2 and RQ3 represent the "Knowledge Base" part, offering applicable knowledge and enhancing the rigor of the research (depicted in Fig. 1 and within the next section).

3. The systematic literature review

3.1. An ontological framework for BC

To build the BC ontology the research work defined by Ref. [19] is mainly used to model the business continuity playground. This framework considers organizational strategies, structure, culture, and established business processes to evaluate business requirements. Additionally, it factors in the current technological infrastructure, applications, communication systems, and development capacities. The aim is to provide a comprehensive understanding of the business need or "issue." By framing research activities to address these business needs, the research is made more relevant and impactful [19].

Given such a clear and consistent business need, IS (Information Systems) research is conducted in two stages. Behavioral science approaches research by developing and justifying theories (**foundations** and **methodologies**) that explain or predict phenomena associated with specific business need. Design science approaches research by assessing artifacts aimed at meeting a specific **business need**. These business needs usually result from an appropriate **environment** that serves the **application case** and comprises **human roles**, **organizations** and involved **technologies**. Overall, the goal of behavioral science research is to discover the reality of the situation since theory is briefed by truth, and design is informed by utility [19] (see Fig. 1).

3.2. The design of the BC ontological framework

IT and IS are inextricably linked as critical components in guaranteeing BC. Researchers and IT professionals have long recognized IT's significance in utilizing various methods to improve BC initiatives [20]. IT can be used to reduce downtime - increase uptime and thus contribute to better financial results, because each minute of downtime has a cost. Hence, the most important requirement for BCP is performing IS solutions while using these IT methods [20].

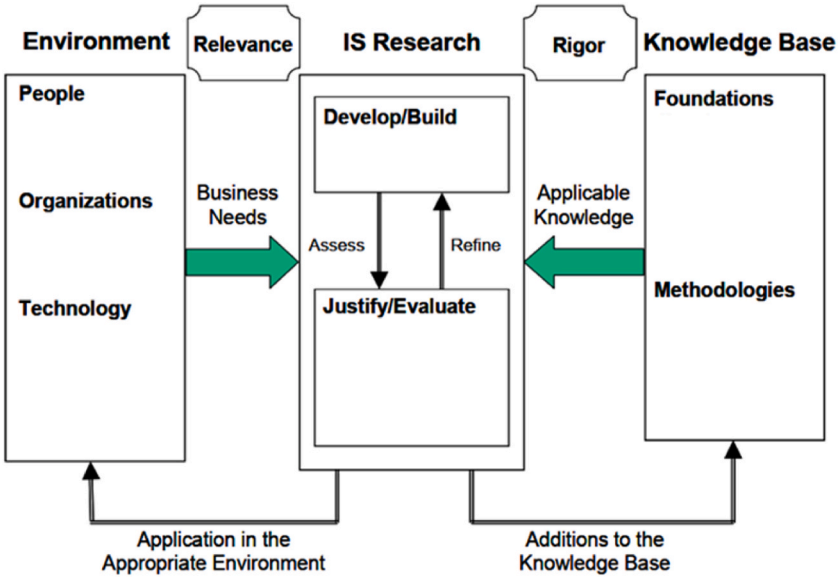


Fig. 1. A sketchy view of the IS research framework defined in [19].

IT and IS are inextricably linked as critical components in guaranteeing BC. Researchers and IT professionals have long recognized IT's significance in utilizing various to improve BC initiatives [20]. For example: IT can be used to reduce downtime - increase uptime and thus contribute to better financial results, because each minute of downtime has a cost. Hence, the most important requirement for business continuity is performing IS solutions [20].

For all these reasons, IS and BC are highly complementary and useful to one another in a variety of ways, including: (i) documenting and continuously annotating the BCP specifications and verifications, (ii) implementing the BCP and connecting its features within the firm's IS, and (iii) testing the BCP and evaluating its efficiency and robustness by troubleshooting the deployed BC features within the IS.

Hence, creating an ontology for assessing the BC was initiated based on the framework explained previously. In fact, we have considered various ontology development approaches, such as UPON [21], UPON lite[21], NeOn [22], and Ontology 101 development [23], for speeding up the ontology engineering process. In detail, (a) our ontology was built from scratch, (b) it's a single ontological format and does not merge two or more ontologies, (c) it's formed manually referring to the IS research framework but enriched automatically, and (d) the concepts of the ontology are the papers' keywords and thus these are previously retrieved and classified manually in order to satisfy the notion of consistency in the BC topics.

While using an established Information Systems (IS) research paradigm to design a Business Continuity (BC) ontology, a divergence in methodology is visible. An exhaustive search was carried out, including SCOPUS and Web of Science (WoS) through a sweeping research query **"business continuity"**, revealing different data on publication origins, years, and WoS categories. Furthermore, an examination investigated the complex connection between crisis circumstances, such as Japan's seismic disasters and the Fukushima incident, and the development of BC research questions. The new approach sheds light on the multifaceted interaction between various crisis situations and theme focus within BC planning. This study differs in that it integrates complete data and provides insights into how crisis circumstances affect and influence the path of research questions.

The information for this analysis was gathered from almost 2600 articles with the goal of deepening understanding of the domain. Following that, the research papers were analyzed and all key words extracted to serve as concepts for the designed ontology. As a result, a preliminary BC knowledge graph was produced. This includes the article's concepts or "topics," authors, article types (journals, meetings, books, etc.), and publication locations. Topics are linked to other topics based on their frequency of occurrence. We also know how many times each topic has been mentioned (that is, the number of papers). The title, summary, DOI, and contributors are also included in the graphic.

3.3. The implementation of the BC ontological framework

The implementation of the BC ontological framework introduces several innovative aspects to the management of BC dynamics. The implemented ontology's class hierarchy primarily consists of IS research framework classes and subclasses, with the retrieved paper topics serving as concepts. This ontological framework uniquely addresses gaps in existing models by explicitly categorizing relationships between BC concepts and their relevance to business needs, resilience strategies, and BC-specific risks. In particular, it

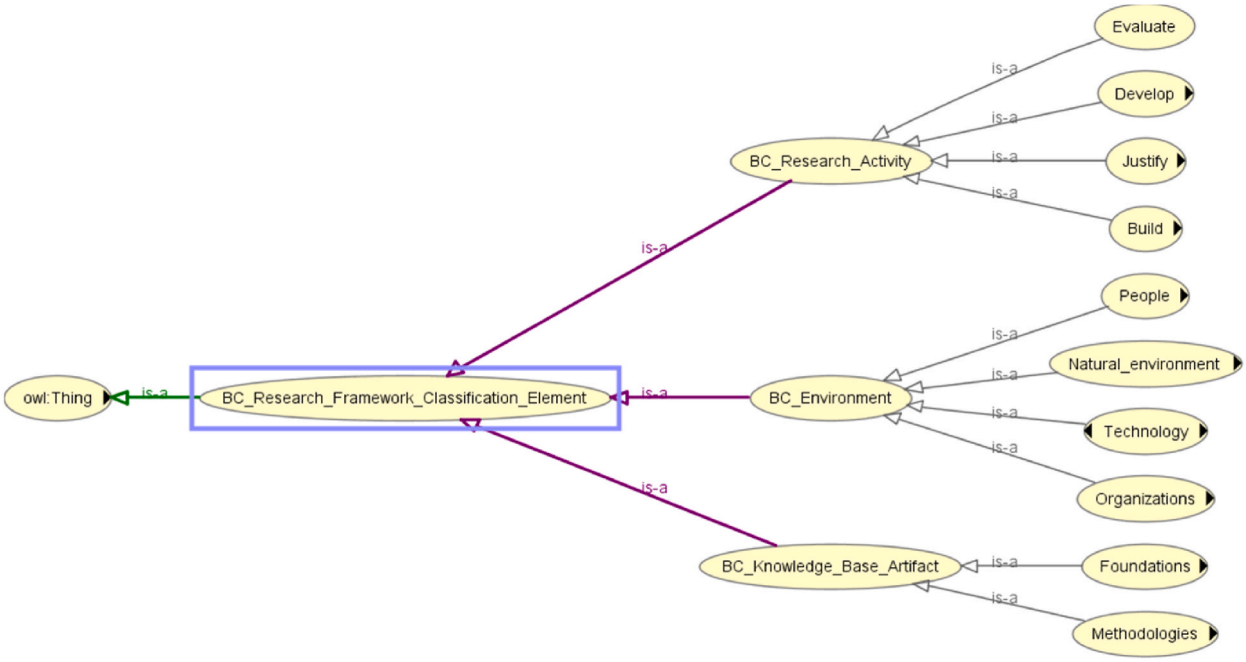


Fig. 2. Upper level concepts of the BC ontology depicted as a graph and visualized with OWLViz

also integrates key components of the BC environment—such as organizations' crisis response protocols, technological threat detection systems, and human elements like emergency communication and evacuation procedures. These aspects are essential for ensuring operational continuity in practice. For example, hierarchal properties were implemented such as: papers "***has_Author/has_Type***" or "***concerns***" some topics, topic "***is_Related_To; provides_business_needs_to*** or ***provides_rigor_to***" other topics, and other relationships.

After categorizing the concepts within the ontology, the model also supports real-time dynamic queries of BCenvironments, enabling advanced predictions of potential disruptions and scenario planning. For instance, it can detect incoming threats through technology-based systems or process government announcements that impact organizations and people during emergencies, ensuring that BC plans are continuously adapted. This innovative aspect allows for rapid adjustments to new information, such as real-time feedback from BC incidents, which earlier models did not adequately capture. The ontology further enhances decision-making by facilitating instant access to related documents and scenarios, empowering decision-makers to respond quickly to emerging threats.

The ontology has four layers and is accessible for evaluation here: https://tinyurl.com/4pc2ejkf. Fig. 2 shows the OWL visualization of the first two layers of the implemented ontological framework for the BC. It portrays the classes and their relationships within the first two layers. In fact, OWLViz is built to work with the protégé owl-editor; it allows class hierarchies in the OWL (The W3C Web Ontology Language) ontology to be viewed and incrementally navigated, allowing comparison of asserted and inferred class hierarchies. This model also addresses the BC environment by integrating organizational structures and technology for evacuation drills and real-time crisis handling, which are key human and technological elements that ensure resilience during a crisis. **This visual approach is another innovation, promoting transparency and ease of use when managing BC complexities**, which contrasts with the more abstract models that rely heavily on manual review. A comprehensive examination for source of componential analysis was conducted in order to develop the proposed ontology [24].

Therefore, the literature review that was performed in order to extract information and structure this paper is given by the following steps (as shown in Fig. 3).

1. **The proposed ontology defines the semantics of BC rules, focusing on processes that traditional models overlook** such as emergency communication, handling unexpected threats, and incorporating real-world disruptions into future plans [25]. For instance, it incorporates technology-based threat forecasting, real-time updates from the natural threats, and handling disruptions that impact organizations and people, enhancing the adaptability of BC plans. This semantic structure enhances BC processes by enabling continuous learning and adaptation.
2. **Use of SPARQL query language adds another innovative layer**, allowing for precise data retrieval from the ontology's RDF (Resource Description Framework), which is not commonly integrated in traditional BC models [26]. The RDF is a graph device

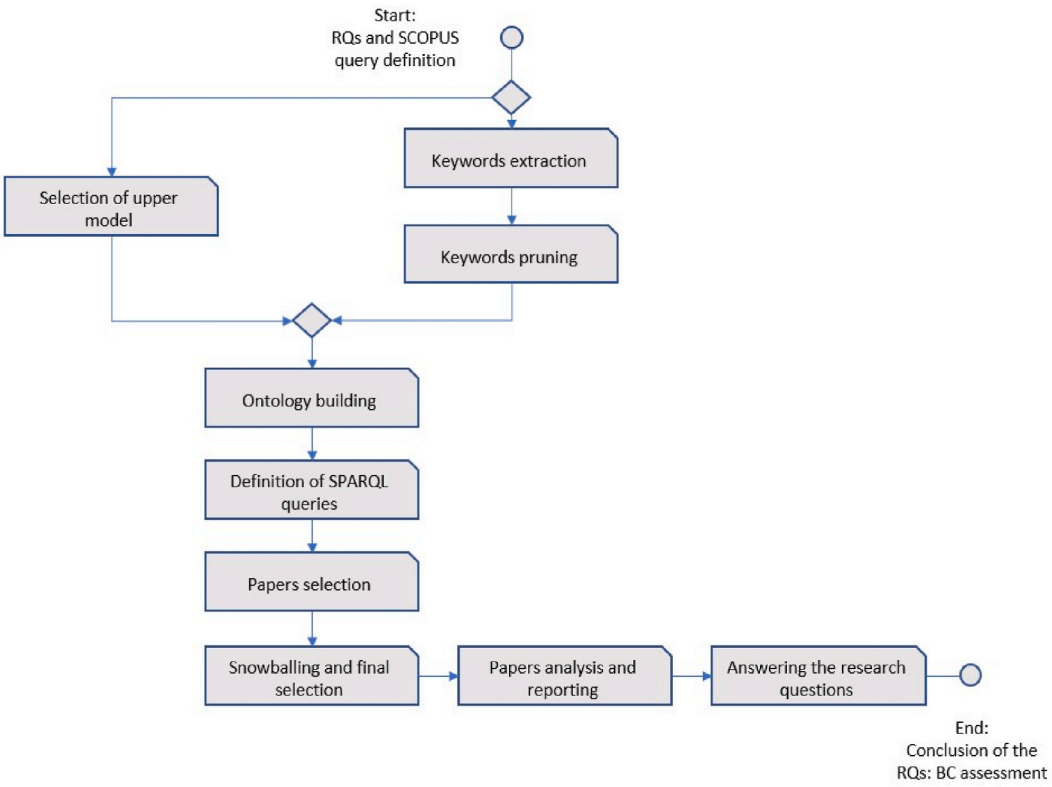


Fig. 3. The systematic literature review process

designed to formally describe Web resources and their metadata, which improves automated BC plan management and enables rapid updates based on incoming data.

3. **Combining the ontological framework with SPARQL for systematic literature reviews (SLR) is an advanced methodology not previously applied in BC models.** This integration allows not only for document retrieval but also the dynamic refinement of BC strategies based on evolving threats and stakeholder needs [27], as shown in Fig. 3.

3.4. The findings of the applied "framework design" methodology

To begin with, chapter 3 of this paper addressed how the ontological framework for BC was addressed and designed. Here, within this paragraph, the outcomes of this "design methodology" are discussed. Later, in chapter 4 of this paper, the "exploitation methodology" that revolves around navigating this BC ontology to extract needed information and knowledge answering the 3 defined research questions is conducted.

Additionally, the ontology was developed and populated using the results of the previous sweeping research query results (papers and keywords) in order to perform the systematic literature (SLR) review for this work. In fact, SLRs are essentially different from traditional literature reviews since they are aimed to address a specific research topic (e.g., 'what works' or 'what works best') by gathering data from the literature. As a result, SLRs do not aim to achieve the same goals as traditional literature reviews, which often include assessing existing knowledge in a given issue domain and finding gaps and topics for future study [28].

Understanding how the BC is currently conceived, which technologies have contributed to shaping its concept, and which are the current challenges for further development are fundamental issues in sustaining the BC ontology development. Ontologies for BC processes are unquestionably a viable means of providing such answers when used for crisis responsiveness, integration, and disambiguation of ground data and information because they represent current knowledge while also enabling the creation of new knowledge since the citation measure is an indicator of the accumulation of knowledge. Creating an ontological framework, as in the case of smart cities in Ref. [27], is a useful thing to do since it enables knowledge sharing, management, reuse, collection, interaction, and reasoning [29].

Hence, the following results were reached.

1. Becoming acquainted with the BC environment, research activities, and knowledge base. Indeed, by classifying concepts within the BC ontological framework, such aspects can be identified, and more information can be extracted using the designed framework. Because the concepts point directly or indirectly to relevant research papers, it is entirely possible to investigate the methods and environment components for the BC in general or within a specific sector.
2. Establishing a BC knowledge base. In fact, all of the classified topics combined with the filled ontological framework, particularly its knowledge base artifacts, form an interesting and complete knowledge base for the BC. The research papers that are linked to the concepts may thus form the various parts of the knowledge base subclasses such as methods, constructs, theories, study cases, and so forth.
3. Identifying threats to business continuity: The threats to business continuity could be easily identified using the accident subclasses of the BC environment components. Pandemics, terrorism, floods, cybersecurity attacks, and other current threats are examples of current threats within the ontology. These threats are critical for assisting in the development of a BCP because the BC process identifies the majority of potential threats to a firm and provides a framework for building resilience and the capability for an effective response that protects the interests of its key stakeholders, notoriety, brand, and wealth creating activities[11].

The following section concerns thus the application of this methodology in order to answer the research questions defined previously in section 1. This will basically go through the literature review steps for each research question to provide explanations and answers to the specific topic.

4. Answering the research questions: the "exploitation" methodology

The following paragraphs provide explanations and steps to formulate conclusions regarding the multi-faceted issues addressed by the research questions RQ1, RQ2, and RQ3. These steps involve executing SPARQL queries, analyzing their results, selecting relevant papers, and reporting and analyzing the findings. Through these processes, conclusions are derived to address the research questions effectively.

In this research work in order to navigate the ontology and retrieve the according papers (step "Defining of SPARQL queries" of the process described by Fig. 3), mainly three types of queries were considered.

1 ***Topic queries:*** They return the papers based on a predefined topic list consisting of papers' keywords. For example: Topic_list = ["Business_continuity_plans","Business_continuity_(bc)","Business_continuity_planning_(bcp)","Business_continuity_managment_(bcm)", "Business_continuity_management_system","Business_continuity_management", "Business_continuation", "Bcm", "Bcp"]

2 ***Taxonomic queries:*** They return the papers based on the topic concepts that concerns a certain class or subclass of the concepts such as BC_environment or BC_foundations for example. This could be "railways" in organizations for instance which is a subclass of BC_environment.

3 ***Refining queries:*** They return the papers based on some specifications such as some relevant words in the abstract, the year of publication, the number of citations, authors, etc.

To further enhance transparency and credibility, the selection process for papers in the systematic review was based on a clear set of inclusion and exclusion criteria.

Examples of inclusion criteria: Peer-reviewed journal articles, Written in English, Addressing BC from environmental, technological, organizational, or human-role perspectives, and Containing empirical data or practical case studies.

Examples of exclusion criteria: Lacked relevance to BC (based on the ontology's domains), were solely theoretical without practical implications, did not provide sufficient empirical evidence or actionable strategies for BC management.

To perform the literature review process, the queries phase was rather composed of the three types of queries in this order.

1. Obtaining the relevant papers from the topic list that is given in the example of the topic queries previously, through performing the ***topic query*** as shown by Fig. 4 below.

2. Obtaining the papers relevant to once concept or more through executing a ***taxonomic query*** as shown by Fig. 5 below.

3. Refining the papers using some refining queries: Once the papers were retrieved using the topics list and the taxonomy of the ontology, some refines were performed basically for classifying the papers per topic in one subclass of the ontology. The output of this process is explained in the next paragraph.

The information extraction process as described previously is finalized by performing some formatting and contextualizing coding techniques that allow making the best use of the information disposal (see Fig. 3). Fig. 6 below describes the steps of generating the report file of the retrieved papers. In fact, two dictionaries are formed to create the file containing the most important topics for one section and its according papers. This file is later alphabetically sorted and used to report the retrieved papers' most important ideas and contributions regarding one specific topic and then summarize them.

In the following subsections, the research questions are treated one by one, starting by RQ1. To each RQ, the corresponding executed query and results are explained along with the selected papers and their reporting and analysis.

4.1. RQ1: to which environmental, technological, organizational, and human-working-role areas BC is applied?

This section seeks to provide **actionable guidelines** for applying Business Continuity (BC) across various domains, namely environmental, technological, organizational, and human-working-role aspects, based on insights derived from the ontological framework (as shown in Fig. 7). The BC environment is composed of roles, technologies, and processes involved in sustaining organizational operations and managing disruptions. For example, in the **environmental domain**, BC can guide responses to natural disasters affecting critical infrastructure like railways or power grids. In the **technological domain**, it can address IT disruptions, such as system failures in banking systems. In the **organizational domain**, BC helps prepare companies for workforce shortages, such as during pandemics. Finally, the **human-working-role aspect** can focus on ensuring that key personnel are trained to manage emergencies, like emergency response teams in hospitals. By understanding how these components interact, organizations can formulate **strategic responses** to enhance their resilience.

4.1.1. Key BC areas and findings

The executed query was performed as explained in the introduction of section 4 (depicted by Fig. 6), following the defined process: topic, taxonomic then refining queries. It refers in this case to the BC_environment class regarding the taxonomic reasoning.

This query returns n = 331 papers and the following number of topics which are mainly keywords of the retrieved papers of each nature. These topics, which refer to a specific subject or domain of knowledge that is represented and structured within an ontology [30], are classified as in Table 1.

In fact, the various areas within the BC environment, such as risk assessment, information and technologies, and societies and

```
queryString = """
            SELECT ?l ?topicConcept
             { ?y a owl:Class .
             ?y rdfs:label "Paper" .
             ?inst a ?y .
             ?inst rdfs:label ?l .
             ?inst a ?restriction .
             ?restriction owl:onProperty ?prop .
             ?prop rdfs:label \"""+ propertyName +"""\" .
             ?restriction owl:someValuesFrom ?topicConcept .
             ?topicConcept a owl:Class .
             ?topicConcept rdfs:label \"""+topic_List[t] +"""\" .
             } order by ?l
    """
```

Fig. 4. The SPARQL Query for retrieving the papers according to topic list

```
queryStringTaxonomicReasoning = """
            SELECT ?l ?topicConcept
             { ?y a owl:Class .
             ?y rdfs:label "Paper" .
             ?inst a ?y .
             ?inst rdfs:label ?l .
             ?inst a ?restriction .
             ?restriction owl:onProperty ?prop .
             ?prop rdfs:label \"""+ propertyName +"""\" .
             ?restriction owl:someValuesFrom ?topicConcept .
             ?parentClass rdfs:label \"""+parentConcept +"""\" .
             ?topicConcept rdfs:subClassOf* ?parentClass .
             } order by ?l
    """
```

Fig. 5. The SPARQL Query for retrieving the papers according to the taxonomy of the Ontology

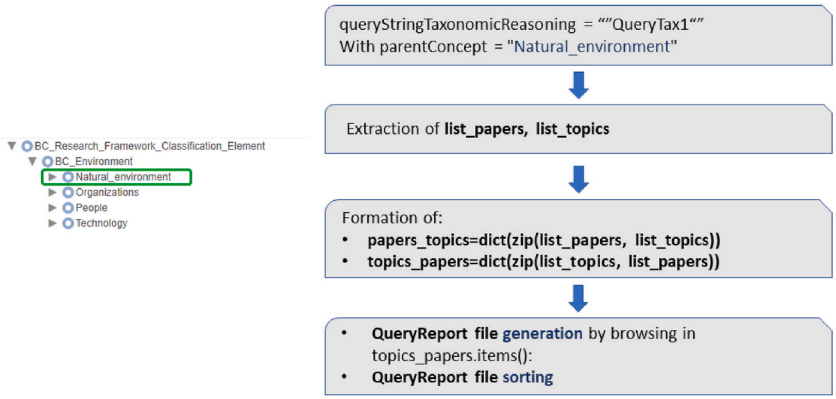


Fig. 6. The class-related report file generation process

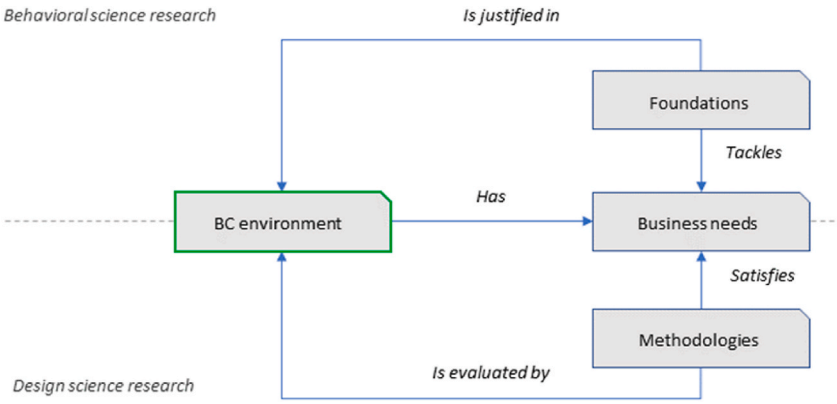


Fig. 7. The relation between the BC environment and the Business needs

institutions, are all essential in preparing for and responding to disruptions. For example, risk assessment helps identify potential disruptions and their impacts, while information and technologies support effective communication and coordination during a disruption. Societies and institutions, on the other hand, provide the necessary infrastructure and support systems to enable effective response and recovery efforts [31].

In turn, disruptions can arise from various causes, such as natural disasters, technological failures, human errors, or deliberate attacks. By addressing each of these causes in a comprehensive and integrated manner, organizations can build resilient BC environments that are better equipped to withstand and recover from disruptions. This is why the various areas within the BC environment are interrelated and interdependent, and must be approached holistically in order to achieve effective BC outcomes [31].

Table 1
Obtained results by area of research for each RQ.

Area of research	Query Results	Topics description
RQ1		
• **Natural threats** • **People** • **Technology** • **Organizations**	mt1 = 62 topics mt2 = 87 topics mt3 = 139 topics mt4 = 232 topics	The last year has demonstrated the need of risk management and emergency response planning in a variety of contexts, including the natural threats, people, and technology. This involves handling issues like influenza, earthquakes, environmental protection, cyber-attacks, and technological failures. Organizations have had to change their strategy to meet these risks and their impact on essential infrastructure, healthcare, and the economy. Overall, comprehensive risk management is required to handle the numerous dangers to the environment, people, and technology.
RQ2		
• **Constructs** • **Frameworks** • **Instantiations** • **Instruments** • **Methods** • **Models**	mt1 = 64 topics mt2 = 16 topics mt3 = 20 topics mt4 = 12 topics mt5 = 34 topics mt6 = 11 topics	To address these issues, a variety of frameworks have been established, including the Analytic Hierarchy Process, Business Continuity Management Systems, Business Continuity Planning and Conceptual Framework, and computer and data center networks. To collect and process information, numerous instruments are used, including computer hardware, embedded systems, industrial control systems, data storage devices, and health surveys.
RQ3		
• **Data analysis techniques** • **Formalisms** • **Measures** • **Validation criteria**	mt1 = 12 topics mt2 = 33 topics mt3 = 36 topics mt4 = 15 topics	Data analysis techniques including data gathering, categorization, analytics, mining, processing, reduction, transmission, and visualization are critical for recognizing and comprehending hazards to an organization's assets and activities. Measures such as service continuity, data integrity, privacy, replication and security, digital forensics, preservation and storage, disaster response and resilience, economic impact, and interdependence are critical for evaluating the effectiveness of risk management and BCP.

4.1.2. Guidelines and recommendations for BC application

To be able to solve RQ1, the papers were selected according to the most important topics which are mostly related to.

- ***Covid-19, influenza, earthquakes, environmental protection and carbon reduction*** for Natural threats.
- ***Business roles (managers, owners, etc.), cyber-attacks, diseases, emergencies, healthcare*** for People.
- ***Technical and computer accidents, advanced technologies, cloud and communication technologies, emergencies and informational assets, and IT services*** for Technology.
- ***Business management strategies, commercial and corporate aspects, critical infrastructures (railways, energy networks, etc.), disaster management and recovery, emergencies, healthcare organization, and economical aspects (growth, losses, etc.)*** for Organizations.

The importance of these topics is determined by their frequency in the query results. Hence, we selected between 5 and 6 individual topics or combined topics to address RQ1. The selection criteria for topics to answer RQ2 and RQ3 follow the same pattern.

4.1.3. Strategic insights for managing BC components

- ***Regarding the "natural threats":***

The natural threats is described as a set of natural occurrences, characteristics, and events [32]. At a BC level and when considering the possible strategic consequences of climate change or various natural catastrophes, it may also be designated as a key stakeholder [33].

On one hand, in this section the topic representing natural threats, such as Influenzas and, recently, covid-19 [34], are aspects of the threats and crucial to BC. Tay et al. [35] demonstrates the significance of a set of workflow metrics, disciplined yet prudent personal protection equipment protocols, and clear strategic goals in order to continue managing a significant proportion of patients in the otolaryngology-head and neck surgery service in a safe environment for patients and caregivers. Otolaryngology teams worldwide should seize any opportunity to make organizational and procedural decisions that affect the safety and continuity of services in their jurisdiction, with the goal of staying one step ahead of the pandemic curve. Another work done by Hennessey et al. [36] explains how leaning and disinfection protocols have been developed for products that need to be moved to maintain business continuity. model cleaning procedure provides a template for how individual companies or locations can adapt these procedures to their specific needs.

On the other hand, the environmental protection and the decarbonization methods and techniques play an essential role in the

relation between the natural threats and BC. In fact, the work done in Gasbarro, Iraldo, and Daddi [37] gives an overview of how reduced/disrupted production capacity and inability to do business, or business continuity, correspond to climate-induced physical risk; reduced demand for goods/services corresponds to changing consumer behavior; and reduced stock price (market valuation) corresponds to reputation risk. Finally, increased operational costs are associated with regulatory risk such as emission reporting obligations, fuel/energy taxes and regulations. In summary, physical changes pose the main threat to business continuity, while changes in demand for goods/services and the introduction of new products/services align with market changes, and fluctuations in market valuation align with reputation drivers. Consequently, regulatory drivers align with changes in operational cost and investment opportunities [37].

- ***Regarding the "people":***

The people in this research work could be either the staff (managers, workers, engineers, medical personnel, etc.) or the people receiving the services or the products of one organization such as customers or patients in the case of healthcare organizations [38].

The model developed in Vojtko, Rolínek, and Plevný [39] was built on an analysis of empirical data from 554 crises from 183 Czech companies, with the main goal of identifying the co-occurrence of different types of crises and how managers dealt with them. The application of such a model focused on manufacturing firms, including its calibration, is demonstrated further through a case study of a real company and related scenario analysis. This analysis could be very useful for the manager, for example, to predict the potential consequences of various managerial decisions when a certain type of crisis occurs, allowing them to avoid causing further problems in the future. A model like this can be used as a decision support tool for managers dealing with various crises, as well as a means of explaining crisis dynamics.

Moreover, aside from natural disasters mentioned previously in the "natural threats subsection", there are man-made disasters. Human-caused disasters occur when human actions cause various types of infrastructure threats. These types of disasters, whether intentional or unintentional, can cause massive harm to the public. Hence, since it is no longer a question of managing the crisis from the point of view of continuity, but rather of the causes/origin of the crisis. One could also classify these crisis occurrences according to the timing of the events: cause of the crisis, identification of the crisis and launch of the alert, management of the crisis, learning from the crisis, and so on. Furthermore, they are sometimes directed by people or organizations to gain hidden benefits, and they may be influenced by religion or belief. The 9/11 attack was a disaster in which 19 Al-Qaida terrorists hijacked four planes and intentionally crashed them into the World Trade Center Twin Towers and Pentagon, killing all passengers and approximately 2976 people in the buildings. The Sasser worm is yet another man-made disaster that affects computers running Microsoft operating systems [40].

As per Hom and Chous [41], it's very likely that there will be an outbreak of influenza in the future. Epidemiologists and business consultants are warning about the possibility of an outbreak. That makes it important to pay attention to these warnings since our livelihoods may be affected [42]. This research work focuses on the involvement of people in crisis management, including staff, customers, and patients. Models are developed to analyze crises and assist managers in decision-making, highlighting the importance of considering the needs and roles of individuals in ensuring BC and effective CI management.

- ***Regarding the "Technology":***

The technology in this research study is outlined as the developed and under-development technologies, which are largely ICT, and their integration into users' personal and professional lives [43].

As mentioned in Manning [44], proof testing against all possible outcomes becomes increasingly difficult as complexity grows inexorably. Risk management methods used in systems engineering and process continuity assurance must be extended beyond their current macro domains all the way down to the micro level. As a result, risk and impact analysis techniques, as well as potential failure mode assessment and avoidance and prevention planning, has to become an integral part of all engineers' basic knowledge.

On this same basis, the work proposed in 2021 by Bennett and McWhorter [45] aims at explaining VHRD (Virtual Human Resource Development) role in the maintaining of the BC within many organizations while and after the covid-19 crisis. In fact, with technology so critical to business survival and education throughout the epidemic, the globe needed VHRD. VHRD has progressed from the margins to the heart of organizational practice. Many new companies and professions were thrown into the realm of VHRD in the year 2020 to accommodate work-from-home mandates and alternative work tactics [46]. The epidemic resulted in a new split between necessary and non-essential personnel, sanitation practices, layoffs and decreased hours, supply chain disruption, quick innovation, and other changes. In retrospect, the world ended with a schism between the pre and post covid-19 historical periods. Virtual recruiting and onboarding, for example, become essential components of pandemic VHRD to keep the economy and corporate operations running [45].

Furthermore, by using resource pooling, it's possible to avoid the need for additional physical servers when implementing new services over a long period of time, which is a significant investment [47]. And as exploited by a use case concerning e-learning in Kenya by Kihara and Gichoya [48], many options exist with cloud computing technologies, including disaster recovery, business continuity, data consolidation, availability, confidentiality, and data integrity. Consequently, users are not required to set up a data backup and disaster recovery solution to ensure data security and business continuity. In fact, utilizing cloud storage, there is no need to be worried about the type of storage devices included, the interface and protocol used, the connecting medium between storage and server, and so on, as if each storage device were utilized individually according to the feedback in Tang [49].

Regarding emergencies and informational assets, according to the research done in Pingel et al. [50], a BCP should consider at least: (a) the critical functions of an organization, (b) the critical staff, (c) the alternative staff to serve as a backup in the case of a crisis, (d)

the critical resources and their backup, (e) the communication guidelines and templates, and (f) the special equipment for emergencies. As (d) and (f) are relative to technology deployment within the company, it's thus clear that technological assets play an important role for the BC.

Overall, Technology is essential for business continuity, enabling remote work, efficient data storage, and reliable IT systems through virtual human resource development, cloud computing, and IT continuity management. Assessing risks, considering previous activities, and implementing risk management frameworks are essential for leveraging technology effectively in BC.

- ***Regarding the "Organizations":***

An organization is a structured collection of human and physical resources who coordinate their activities and cooperate to achieve goals, such as corporations, government departments, healthcare institutions, universities, research centers, banks, and so on [51]. From a BC perspective, the term "Organization" can be better understood by dividing it into the following key components.

1. Processes/Operations:
   Processes refer to the internal workflows, roles, and responsibilities employees perform, including the hierarchy, division of work, and coordination within and between departments. For example, Mongioi, McNally, and Thompson [52] highlight how companies enhance BC through partnerships, such as private and public sector collaboration to strengthen emergency preparedness.
2. Premises:
   The physical facilities of an organization are crucial to BC. The relationship between the BCM and an organization's infrastructure can be illustrated by its electrical architecture, where efficient design, supervision control systems, and BCM practices ensure the continuous operation of the facilities while minimizing maintenance and energy costs [53]. This includes updates to system architectures that prevent disruptions and enhance security, as Dimov and Tsonev [54] demonstrate in the context of operating system updates.
3. Providers:
   Providers, including external partners, suppliers, and service providers, are vital for ensuring an organization's continuity. Safeway, a national grocery chain, serves as an example of a private partner ensuring business continuity in the transportation sector during emergencies [52].

Critical infrastructures are an interesting case in regard to BC. In fact, in such infrastructures, beyond significant financial losses, the potential implications of cyber threats for example include disruptions to BC, data loss, reputational injury, loss of future competitive advantage, and hostility from partners and consumers [55]. These disruptions are particularly important since findings of the vulnerability assessment can be used as input for BC and maturity assessments [56]. As a result, the efficiency of the architecture, supervision control systems, and business continuity management (BCM) improve the quality and safety of the services while allowing management of the operation, maintenance, and energy costs [53].

In a nutshell, the concept of business continuity (BC) is vital for organizations across various sectors. Partnerships between private and public entities can strengthen emergency preparedness and ensure commercial continuity. Innovation, driven by customers, new technologies, and socio-environmental sustainability, plays a significant role in market developments and BC. Effective electrical architecture, supervision control systems, and BCM enhance service quality, safety, and management of operations and energy expenses. Critical infrastructures face cyber threats that can lead to financial losses, data loss, reputational damage, and other disruptions, emphasizing the importance of vulnerability assessments for BC.

4.2. RQ2: what are the BC foundations and its most relevant examples?

The BC foundations can be defined as any concept or fact related to BC [57]. These foundations in the case of BC tackle the BC needs

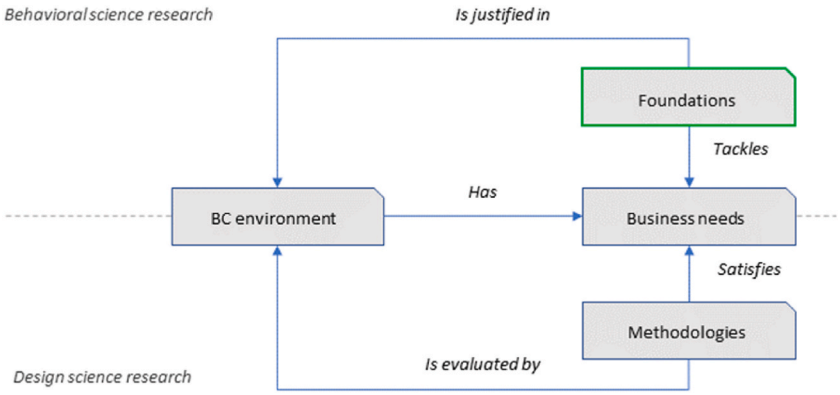


Fig. 8. The relation between the BC foundations and the Business needs

as they outline crucial components and resources that are necessary to an organization's business needs as shown in Fig. 8 below.

4.2.1. Key BC areas and findings

The executed query was performed as explained in the introduction of section 4, following the defined process: topic, taxonomic then refining queries. It refers in this case to the BC_foundations class regarding the taxonomic reasoning.

This query returns n = 174 papers and the following number of topics which are mainly keywords of the retrieved papers of each nature. These topics are classified in Table 1.

4.2.2. Guidelines and recommendations for BC application

In order to answer RQ2, the papers were selected according to the most relevant topics which are basically related to.

- ***Safety design, Hardware*** *(physical systems or devices supporting the overall BC framework: servers, networking equipment, and so on)* ***and software facilities, Information security, knowledge engineering*** for Constructs.
- ***Analytic hierarchy process (ahp), BCMS, BCP, conceptual framework, Computer and data center networks*** for Frameworks.
- ***Computer applications, cryptography, documentation, geographical distribution, e-learning and intelligent systems*** for Instantiations.
- ***Computer hardware*** *(specific tools or devices used during BC operations, such as backup generators and data recovery systems, highlighting)****, embedded systems, industrial control system, data storage equipment and health survey*** for Instruments.
- ***Business impact analysis and assessment, computational and data handling methods, information analysis, prevention methods, and failure and factor analysis*** for Methods.
- ***Knowledge based systems, knowledge acquisition, conceptual modeling and business models*** for Models.

4.2.3. Strategic insights for managing BC components

- ***Regarding the "Constructs":***

A construct could be a notion or theory that has numerous conceptual parts, usually one that is deemed subjective and not founded on scientific evidence [58].

The main objective of evaluating disaster recovery is to support a long-term plan for constructing a data center and facilities that ensure BC [59]. Today, people prioritize family and employment and value a flexible work environment. The work in our sector mainly involves computer-based tasks, making physical location less relevant [60].

Similarly, constructs such as data centers, which process sensitive and vital corporate information, require both physical and logical safeguards to ensure information system security. Implementing an ISMS (Information Security Management System) can aid in identifying, managing, and reducing information security threats in the data center and provide overall protection for these constructs [61]. As a result, the ISO 27001 ([62]:2005) regarding ISMS and the BS 25999 [63] about BCMS are two standard management systems that can be characterized by a Deming cycle, which consists of a closed loop. Although there are considerable differences between the two systems, the Deming cycle looks to be similar to the technical control loops of DES theory [64]. Eventually, and for this particular purpose, a critical part of supporting business continuity is the capacity to relocate services offered from affected sites to unaffected areas while satisfying their resource requirements during a disruptive event. This type of rerouting is known as recourse [65].

Afterall, constructs, subjective notions lacking scientific evidence, have multiple conceptual parts. Disaster recovery evaluation supports data center construction for BC. Flexible work environments prioritize family and employment. Data centers require physical and logical safeguards via ISMS implementation. ISO 27001 and BS 25999 utilize a Deming cycle. Recourse enables service relocation during disruptions. Updated business continuity practices protect sensitive information and foster organizational success.

- ***Regarding the "Frameworks":***

Frameworks are mainly a fundamental generic structure that underpins a certain system or a notion. They are mainly used to enable the building of several applications from a single structure or (sub)domain [66,67].

One of the frameworks in regards with BC is about a multi-criteria decision making and analytical hierarchy approach with expert choice software was employed by Ref. [68]. This research intends to develop recommendations that will assist the university's stakeholders in making the optimal selection when selecting a backup recovery approach for a BCP so that it reduces the risks posed by a disaster.

From another perspective, during covid-19 several technical-framework related issues affected the BC as stated in Papagiannidis et al. [69]. In fact, normal capacity management techniques would not have forecast the crisis-induced change in usage. In large organizations, teams with representation from all functions would have been more effective in dealing with the looming dilemma, as teleworking is not simply an ICT infrastructure issue, but also touches on human resource management. Similarly, in order to improve security and BC, a security system can be implemented in a large-scale data center, along with additional measures to enhance immunity against cyber threats. This can help detect and respond to various cyber threats such as malware, trojans, spam, and others in a flexible and efficient manner using security firewalls [70].

Finally, frameworks provide foundational structures for systems or concepts, enabling the development of multiple applications. Multi-criteria decision-making aids in optimal backup recovery selection for business continuity. Covid-19 highlighted technical

framework challenges, requiring cross-functional teams for teleworking. Implementing security systems enhances data center immunity against cyber threats. Recent advancements emphasize the need for BC based on cloud computing solutions. Server platforms are vital for "always-on" computing environments.

- ***Regarding the "Instantiations":***

The instantiation principle is the representation or symbolization of a certain theory or foundation and may be applied to a broad range of models, including example and abstraction models [71].

An instantiation for BC applications could be the prototype designed in Xiong, Jia, and Liu [72]. In a virtualization setting, their prototype makes extensive use of techniques such as application-level state recording and rollback, backward/forward taint tracking, and infection quarantine. The real-world incursions and benchmarks are considered to assess the prototype's recovery performance and thus enhance the BC.

Another case for instance could be the ability of cloud computing in altering and automating the operations of a country's public and private Higher Learning Institutions described for the case of Kenya by Kihara and Gichoya [48]. In fact, cloud computing technology provides several benefits such as disaster recovery, data handling, business continuity and so forth.

In a nutshell, the instantiation principle represents theories or foundations and applies to various models. A BC instantiation example is a virtualization prototype using application-level state recording, taint tracking, and quarantine techniques to enhance recovery performance. Cloud computing can automate operations in Higher Learning Institutions, providing benefits like disaster recovery and business continuity. Cybersecurity is crucial for BCP, involving the entire organization and not just the IT department. Failure to defend against environmental risks is a management oversight.

- ***Regarding the "Instruments":***

An instrument, in general, could be a means or a way of achieving something. For example, simulation tools, as a type of instrument, can be used to validate models and test certain methodologies or frameworks [73], such as interfaces. Since the interface between industrial control systems and the outside Internet environment via IoT technology, information and communication technology is vulnerable to both physical and cyber-attacks as it is connected to the grid [74]. Cyber-attacks frequently result in many dangers that impact infrastructure and business continuity; in certain circumstances, human people are also harmed. Therefore, in an IoT-based Smart Grid communication environment, the research work in Yin et al. [74] suggests a Cybersecurity Solution based on IDS that is able to identify threats in real time. Consequently, BC requirements, storage infrastructure consolidation, and post-9/11 regulatory difficulties all contribute to a continuing need for a dedicated storage system with a larger data storage capacity [75].

From another perspective, as stated in Malladi et al. [76], since egg production facilities sometimes lack the ability to store eggs for extended periods of time, such disease control procedures may affect business continuity and have an influence on food security. This research work suggests using a holding time before egg movement in combination with targeted active monitoring as a novel technique to moving eggs from flocks inside a control region with a low risk of HPAI virus contamination.

Finally, instruments like simulation tools validate models and enhance frameworks. Increased storage capacity is needed to meet BC requirements. Feedback control loops improve information security policy implementation. Novel techniques, such as holding time and targeted monitoring, address disease control and ensure business continuity.

- ***Regarding the "Methods":***

A method could be a certain way of accomplishing endeavors such as a critical risk analysis in the context of security concerns [77]. Risk analysis must consider business views, which might include indicators such as financial Impact, reputation, critical level, organization size, and organizational type [77]. Therefore, FTA and ETA combined methods may be utilized to construct conceptual model linked business impact and aspects [77]. In fact, BIA (Business Impact Analysis) was introduced to ensure property protection and business continuity in new building design, with or without insurer participation. The British Standard for fire engineering needs improvement to include business protection objectives. The Technical Committee responsible for the standard supported this idea and drafted PD 7974-8 to address property protection, mission continuity, and resilience in building design [78].

Similarly, expanding storage and BC requirements; high-bandwidth, low-latency SAN requirements; storage infrastructure consolidation; and post-9/11 regulatory difficulties are some of the causes driving this trend [75]. investigate network traffic in a planned metro WDM ring design SAN with variable-length packets. In the same context, data analysis and visualization techniques come along with decision making, as after constructing a data warehouse, a company may use structured and unstructured data to capture information about consumer interactions. The goal is to turn this data into valuable information for decision-making, particularly in communities where an effective framework for sharing security information is lacking [79]. While most communities understand the procedure for responding to physical incidents, they have little or no system for communication, incident response, business continuity, and disaster recovery in the case of an incident (for example, an attack on a critical computer network). More importantly, they lack a system for exchanging information in order to handle cooperative incidents. Therefore most firms need community security methods to be implemented for protecting their data and thus the BC within the organization [80].

Finally, methods like risk analysis, business impact studies, and integrating risk assessment with BIA principles aid in business continuity planning. Data analysis and visualization techniques support decision-making for maintaining business continuity. Community security methods and information sharing systems protect data and ensure business continuity. Evaluating disaster risks and

conducting system simulations facilitate BCP decisions.

- ***Regarding the "Models":***

A model is a simple overview of a system or a process that can be used to enhance understanding or anticipate future outcomes. In fields such as BPM and BC, models are commonly used to help achieve these objectives [81].

In the context of BC, an important cultural feature is to ensure that BCPs are not just treated as decorations on a bookshelf, but are regularly updated. This approach ensures that various company variables, such as changing market trends, modified business functions, technology, or location changes, are reviewed regularly to determine the suitability of existing plans. To support this, staff must be continuously trained and empowered to carry out and support BC initiatives. In summary, effective BC models prioritize the regular review and updating of BCPs and ensure that staff are adequately trained to support these initiatives [82]. The effective modeling of employee talent and profiles can enhance the development of junior employees and retain highly skilled employees in the company. Regular updating a of BCPs is another critical aspect of effective BC model. These measures ensure that changing company variables are accounted for and staff are trained to support BC initiatives [83].

Overall, models enhance understanding and anticipate outcomes in fields like BPM and BC. Effective BC models prioritize regular BCP review and staff training. Modeling employee talent aids in development and retention. Circular business models promote profitability and continuity, crucial during crises like covid-19.

4.3. RQ3: what methodologies have been used for BC? How can we apply them?

The methodologies in case of BC should satisfy the BC needs (see Fig. 9 below) and thus contribute a clearer rules, techniques, measures and criteria in order to determine the accuracy of these needs and to which extent are they met.

4.3.1. Key BC areas and findings

The query was run exactly as described in the introduction of section 4 following the defined process: topic, taxonomic then refining queries. In this example, it relates to the BC methodologies class in terms of taxonomic reasoning.

The query yields n = 96 papers and the number of topics shown below, which are mostly terms from the retrieved articles of each kind. These themes are classified in Table 1.

4.3.2. Guidelines and recommendations for BC application

To answer RQ3, the articles were chosen based on the most relevant topics, which are mostly connected to.

- ***Data acquisition, data classification, data analytics, data mining, data processing, data reduction, data transfer, data visualization, data warehouses and databases*** for Data analysis techniques.
- ***BCM, BCP, Business Process Management (BPM), Business recovery planning, integration facilities and approaches, ISO 22301 and ISO standards*** for Formalisms.
- ***Continuity of services, data integrity, privacy, replication and security, digital forensics, preservation and storage, disaster response and resilience, economic impact and interdependencies*** for Measures.
- ***Benchmarking, Business performance, objectives, success, resilience and sustainability, cost effectiveness, customer satisfaction and efficiency*** for Validation criteria.

4.3.3. Strategic insights for managing BC components

- ***Regarding the "Data analysis techniques":***

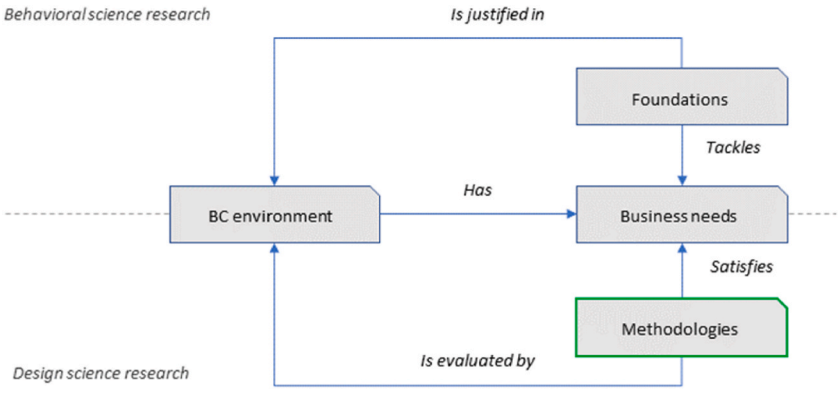


Fig. 9. The relation between the BC methodologies and the Business needs

The use of data analysis to turn unstructured data into structured data was one of the contributions in Liu [79]. This method combines various data formats and helps businesses analyze data to gain new insights, particularly in customer relationship management. Aligning consumers' values with technology enhances promotional activities and technological transfers, improving and maintaining BC [79].

Moreover, advanced backup and recovery solutions that may better meet the more demanding business continuity requirements are highly wanted from a company standpoint. By 2016, one-third of enterprises are predicted to switch backup suppliers owing to cost, administration complexity, and limited capabilities [84,85]. It is also predicted that the corporate distributed system backup/recovery software market would increase to 5.2 billion by 2016, up from 3.8 billion in 2011. As a result, IT management teams must prioritize the development of dependable, user-friendly, and intelligent backup solutions in order to enhance their company competitiveness and market leadership [85]. As a result, a proof-of-concept platform for scalable data mining is given, which enables simultaneous implementations of data mining algorithms on enormous data sets. Several use case studies are highlighted to demonstrate this research's effort on utilizing data mining techniques for effective corporate backup management using big data analytics approaches [85].

Finally, data analysis turns unstructured data into structured data, improving customer relationship management and promoting business continuity. Advanced backup and recovery solutions are sought to meet demanding BC requirements, driving the need for dependable and user-friendly backup solutions. The BCP department should report to an Executive Director for effective organizational-wide change. Telecom hotels and associated facilities support communication and operations for large and small enterprises.

- ***Regarding the "Formalisms":***

Formalisms concern mainly the rules governing the arrangement of various parts or aspects such as the modeling of business processes [86]. BC is concerned with threats that hinder business processes and have a significant impact on operations and revenue. Formalisms address catastrophic occurrences beyond a business model, such as IT loss, staff loss, or extreme weather [87]. For these reasons, in order to ensure effective BCP, it is important to utilize formalisms such as risk and impact assessments. This involves a collaborative effort to identify potential threats to the organization and assess their potential impact. By using these formalisms, businesses can design and implement effective BCPs that address a wide range of potential risks and resulting interruptions [87].

As a result, improved technological approaches (such as CC) can support a resilient SCR even during a crisis pandemic by forecasting the associated risk and planning a timely efficient recovery to maintain BC by adapting to situation-based automated tools for more effective and efficient planning processes. This strategy helps to create a more robust and structured system. [88,89]. In fact, information and communication technologies enable managers to monitor disruptions and facilitate quick recovery of SCs, using formalisms [89,90]. For this reason, managers may now explain how to implement strategies, achieve financial performance, and explore performance results with formalisms such as SCR [91].

Overall, formalisms govern the arrangement of various aspects, such as business process modeling. Formalisms, like risk and impact assessments, are crucial for effective BCP by identifying potential threats and designing suitable plans. Risk-aware business process simulation models assess risk reduction options and improve business continuity. Technological approaches, such as cloud computing, contribute to resilient supply chain recovery and efficient planning processes. Information and communication technologies, along with formalisms, enable disruption monitoring and quick recovery in supply chains. Managers utilize formalisms, like SCR, to implement strategies and achieve financial performance while addressing SCR resilience challenges.

- ***Regarding the "Measures":***

Measures refer to actions taken to reduce or eliminate risks and ensure the continuity of critical business operations in the event of disruptive incidents [92]. In fact, setting a BC strategy ensures that the organization considers the hazards that may hamper the continuation of operations and identifies specific strategies to manage these risks. The BCP gives direction on what measures the business continuity team will take based on the phase of the disaster event, based on the type of disaster event and the amount of work committed [92]. In this context, the measures that organizations need to take as part of their BC planning include keeping an inventory of essential data and duplicating or scanning important documents that identify the vital systems, data, records, and business functions required to sustain the organization's operations [93].

However, the new EU Regulation measures are three times the length of the 1998 Data Protection Act. Marketers on both sides of the Atlantic will have a two-year transition time to minimize any consequences taken for personal data breaches once the transition period expires. With fines ranging from 2 % to 5 % of annual global sales in a sequential 12-month period, commercial organizations simply cannot afford to disregard these new EU measures, which poses the most serious danger to BC in a decade [94]. To ensure the availability of essential data, a possible solution is to adopt a clustering concept that enables several nodes to operate as a single node in a passive-active mode, sharing resources. This measure is typically implemented for mission-critical services and can be complex and costly. The advantage of a clustering approach is that even if a single node fails, the remaining nodes in the cluster continue to function correctly. The BC team can proceed to classify the data level and determine the critical business activities that require such a measure to be put in place [95].

Overall, measures are actions taken to reduce risks and ensure the continuity of critical business operations. BC strategy considers hazards and identifies specific risk management strategies. Essential measures in BC planning include data inventory, and document duplication. New EU regulations impose fines for personal data breaches, emphasizing the importance of compliance. Adopting a

clustering concept can ensure availability of essential data by sharing resources. Control loops and pre-defined plans like BCP and DRP are crucial for maintaining BC, particularly in extreme circumstances.

- ***Regarding the "Validation Criteria":***

Validation criteria are the proof that something is correct or acceptable in a less critical situation. These criteria form a certain way that emphasizes assessment findings [96]. Creating detailed strategies to respond to unpredictable occurrences, either when they will occur or how they will express themselves, is unlikely to be a useful strategy. Instead, organizations may want to think about ways to improve business resilience throughout the organization. In the context of BC, organizations should prioritize investments and decision-making based on roles and tasks rather than hierarchies. One way to achieve this is through an impact study that identifies essential employee groups, business processes, infrastructure, and data, and considers how to support and scale up when specific situations emerge. This approach allows organizations to establish validation criteria for critical functions and resources, ensuring that they are appropriately protected and recoverable in the event of disruptions [69].

Similarly, to ensure the success of the SC for example, it is important to develop and maintain an organizational culture that prioritizes security and recognizes its importance to BC and operations. This ensures that there is alignment between individual and organizational goals, as well as between individual objectives and performance, and the evaluation and reward system. By doing so, efficiency and security in the SC can be improved and maintained. Therefore, establishing validation criteria that align with the organization's goals and objectives is crucial for the success of operations. [97]. Nonetheless, because the Internet now enables data accessibility and connected services, Smart Grid enterprises have moved to leverage such capabilities. This circumstance results in a complicated architecture in which non-secure systems are combined with existing systems that lack security validation criteria [74].

Finally, validation criteria serve as proof of correctness or acceptability in a less critical situation. Organizations should focus on improving business resilience and prioritize investments based on roles and tasks. Disaster recovery models and validation criteria ensure effective recovery plans and availability of critical services. Aligning security goals with organizational objectives enhances efficiency and security in the supply chain. Smart Grid architectures should incorporate security validation criteria. Analyzing validation criteria can help understand the influence of threat susceptibility and improve the efficacy of security projects.

5. Conclusion, limitations and future works

The rising frequency of crisis events in recent years, resulting from a variety of multiplying risk factors inside our increasingly complex and hyper-connected world especially for Cis and essential services, highlights the critical need for solid BC policies and solutions. While the existing research highlights the importance of BC strategies in the face of these issues, it occasionally overlooks a critical aspect: the varied nature of the humans that comprise organizations. Individuals inside organizations display a wide range of traits, including age, social standing, habits, cultures, and hobbies, which are sometimes overlooked in BC debate.

5.1. Conclusion and Limitations

A key aspect of BC is its ability to maintain the operational integrity of **Critical Infrastructures (CI)**, which are vital for sustaining essential services that societies rely on, such as healthcare, energy, transportation, and communication. CI systems are not only exposed to the same risks as general businesses but are also integral to mitigating the effects of disasters, ensuring the continuity of public services in the face of disruptive events.

In this regard, this article presents the findings of a systematic literature review that included 2547 papers and addressed the main themes listed in Table 1 above. Based on the number of topics covered, the natural threats (RQ1), models and instruments (RQ2), and data analysis techniques (RQ3) were found to be the least explored. In contrast, the examined literature provided more complete treatment of critical technological, organizational, and human-working-role components in BC planning, as well as theoretical and fundamental traits.

One basic way to assess BC is to follow a documented Business Continuity Plan (BCP) and its implementation within the Business Continuity Management System (BCMS). However, this is often not enough, as the BCP must continuously evolve through regular assessment to address changing risks and ensure preparedness. In this regard, ontologies for BC are critical for building a comprehensive understanding of both the organizational and infrastructural components of CI, which are fundamental to societal resilience.

5.2. Future works

At this stage, this work lacks an applicable use-case exploitation such as applying the ontological framework to model a firm's BC environment, its business needs, threats and thus indicators to assess the BCP within the organization.

Thus, future works for this research include the following: (a) the methodology makes use of a pre-existing ontology to create a comprehensive knowledge graph based on BC concepts and entities, (b) this network is then used to derive specific BC assessment metrics based on the connected links described in the ontology, (c) the recommended indicators are then validated by BC experts to ensure their relevance and accuracy, (d) a targeted method, which includes questions, surveys, and analysis, collects data aimed to specific BC indicators, highlighting its practical use, (e) special emphasis is placed on developing specific BC metrics for specialized organizational units, testing their relevance through expert advice, and using tailored inquiries to retrieve relevant metrics. Finally, this entire process results in recommendations for improving organizational resilience, insights from the obtained indicators, and an

overall BCP assessment.

This research contributes by presenting a novel ontological framework that highlights how BC strategies can be tailored specifically to ensure the robustness and resilience of CI systems, which play a critical role in maintaining essential services during crises. The framework not only facilitates the development of BC plans but also enables the identification of threats and the continuous assessment of risk across key sectors such as healthcare, transportation, energy, and communication.

In summary, by linking BC to the protection of CI, this research emphasizes the importance of resilient infrastructure to societal well-being. This connection is crucial, as disruptions to CI can have far-reaching impacts on both businesses and the public, underscoring the need for BC frameworks to support the continuity of essential services during crises.

CRediT authorship contribution statement

Oussema Ben Amara: Writing – review & editing, Writing – original draft, Methodology, Investigation, Formal analysis, Conceptualization. **Antonio De Nicola:** Writing – original draft, Methodology, Investigation, Conceptualization. **Daouda Kamissoko:** Writing – original draft, Methodology, Investigation, Conceptualization. **Frédérick Bénaben:** Writing – original draft, Methodology, Investigation, Conceptualization. **Ygal Fijalkow:** Writing – original draft, Methodology, Investigation, Conceptualization.

Disclosure statement

No potential conflict of interest was reported by the authors.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

[1] Iván González-Márquez, Víctor M. Toledo, Sustainability science: a paradigm in crisis? Sustainability 12 (7) (2020) 2802, https://doi.org/10.3390/su12072802.
[2] Helmut Haberl, Dominik Wiedenhofer, Stefan Pauliuk, Fridolin Krausmann, Daniel B. Müller, Marina Fischer-Kowalski, Contributions of sociometabolic research to sustainability science, Nat. Sustain. 2 (3) (2019) 173–184, https://doi.org/10.1038/s41893-019-0225-2.
[3] Anne Jerneck, Lennart Olsson, Barry Ness, Stefan Anderberg, Matthias Baier, Eric Clark, Thomas Hickler, Alf Hornborg, Annica Kronsell, Eva Lövbrand, Johannes Persson, Structuring sustainability science, Sustain. Sci. 6 (1) (2011) 69–82, https://doi.org/10.1007/s11625-010-0117-x.
[4] Thomas Elmqvist, Erik Andersson, Niki Frantzeskaki, Timon McPhearson, Per Olsson, Gaffney Owen, Kazuhiko Takeuchi, Carl Folke, Sustainability and resilience for transformation in the urban century, Nat. Sustain. 2 (4) (2019) 267–273, https://doi.org/10.1038/s41893-019-0250-1.
[5] Laura Petersen, Emma Lundin, Laure Fallou, Johan Sjöström, David Lange, Rui Teixeira, Alexandre Bonavita, Resilience for whom? The general public's tolerance levels as CI resilience criteria, International Journal of Critical Infrastructure Protection 28 (2020) 100340, https://doi.org/10.1016/j.ijcip.2020.100340.
[6] Roberto Setola, Eric Luiijf, Marianthi Theocharidou, Critical infrastructures, protection and resilience, in: R. Setola, V. Rosato, E. Kyriakides, E. Rome (Eds.), Managing the Complexity of Critical Infrastructures: a Modelling and Simulation Approach, Studies in Systems, Decision and Control, Springer International Publishing, Cham, 2016, pp. 1–18.
[7] Nezih Altay, Walter G. Green, OR/MS research in disaster operations management, Eur. J. Oper. Res. 175 (1) (2006) 475–493, https://doi.org/10.1016/j.ejor.2005.05.016.
[8] C.A. Peterson, Business Continuity management & guidelines, in: Proceedings of the 2009 Information Security Curriculum Development Annual Conference, InfoSecCD'09, Kennesaw, GA, 2009, pp. 114–120.
[9] N. Bajgoric, Y.B. Moon, Enhancing systems integration by incorporating business continuity drivers, Ind. Manag. Data Syst. 109 (1) (2009) 74–97, https://doi.org/10.1108/02635570910926609.
[10] M. Niemimaa, Interdisciplinary review of business continuity from an information systems perspective: toward an integrative framework, Commun. Assoc. Inf. Syst. 37 (2015) 69–102, https://doi.org/10.17705/1cais.03704.
[11] Jonathan Reuvid, The Secure Online Business Handbook: a Practical Guide to Risk Management and Business Continuity, Kogan Page Publishers, 2006.
[12] C. Castillo, Disaster preparedness and business continuity planning at boeing: an integrated model, J. Facil. Manag. 3 (1) (2005) 8–26, https://doi.org/10.1108/14725960510808365.
[13] C. Stucke, D.W. Straub, R. Sainsbury, Business Continuity Planning and the Protection of Informational Assets, Taylor and Francis, 2016.
[14] Anon, ISO 22301:2019(En), Security and Resilience — Business Continuity Management Systems — Requirements (2019).
[15] R. Koen, R. Von Solms, M. Gerber, ICT readiness for business continuity in local government, in: 2016 IST-Africa Conference, IST-Africa 2016, Institute of Electrical and Electronics Engineers Inc, 2016.
[16] M. Dey, Business continuity planning (BCP) methodology essential for every business, in: 2011 IEEE GCC Conference and Exhibition, GCC 2011, 2011, pp. 229–232. Dubai.
[17] K. Mano, H. Inomo, W. Shiraki, C. Isouchi, A business continuity plan support system for disaster prevention learning, in: 2012 International Conference on Information Technology Based Higher Education and Training, ITHET 2012, Istanbul, 2012.
[18] F. Gibb, S. Buchanan, A framework for business continuity management, Int. J. Inf. Manag. 26 (2) (2006) 128–141, https://doi.org/10.1016/j.ijinfomgt.2005.11.008.
[19] Alan R. Hevner, Salvatore T. March, Jinsoo Park, Sudha Ram, Design science in information systems research, MIS Q. 28 (1) (2004) 75–105, https://doi.org/10.2307/25148625.
[20] N. Bajgoric, Information technologies for business continuity: an implementation framework, Inf. Manag. Comput. Secur. 14 (5) (2006) 450–466, https://doi.org/10.1108/09685220610717754.

[21] Antonio De Nicola, Michele Missikoff, Roberto Navigli, A software engineering approach to ontology building, Inf. Syst. 34 (2) (2009) 258–275, https://doi.org/10.1016/j.is.2008.07.002.
[22] Asunción Gómez-Pérez, Mari Carmen Suárez-Figueroa, Neon Methodology for Building Ontology Networks: a Scenario-based Methodology, vol. 8, 2019.
[23] Natalya F. Noy, Deborah L. McGuinness, Ontology Development 101: a Guide to Creating Your First Ontology, vol. 25, 2001.
[24] Abdullah Alshehab, Naser Alazemi, H.A. Alhakem, Semantic integration sharing for egovernment domains ontology: design and implementation using owl, J. Theor. Appl. Inf. Technol. 97 (2019) 1820–1831.
[25] Janusz Zawiła-Niedźwiecki, Business continuity, Found. Manag. 2 (2) (2010), https://doi.org/10.2478/v10238-012-0031-x.
[26] Antonio De Nicola, Michele Missikoff, A lightweight methodology for rapid ontology engineering, Commun. ACM 59 (3) (2016) 79–86, https://doi.org/10.1145/2818359.
[27] Antonio De Nicola, Maria Luisa Villani, Smart City ontologies and their applications: a systematic literature review, Sustainability 13 (10) (2021) 5578, https://doi.org/10.3390/su13105578.
[28] Sebastian Boell, Dubravka Cecez-Kecmanovic, On being 'systematic' in literature reviews in IS, J. Inf. Technol. 30 (2015), https://doi.org/10.1057/jit.2014.26.
[29] Theresa Edgington, Beomjin Choi, Katherine Henson, T.S. Raghu, Ajay Vinze, Adopting ontology to facilitate knowledge sharing, Commun. ACM 47 (11) (2004) 85–90, https://doi.org/10.1145/1029496.1029499.
[30] Bahram Amini, Roliana Ibrahim, Mohd Shahizan Othman, Mohammad Ali Nematbakhsh, A reference ontology for profiling scholar's background knowledge in recommender systems, Expert Syst. Appl. 42 (2) (2015) 913–928, https://doi.org/10.1016/j.eswa.2014.08.031.
[31] Andrew Hiles, Business Continuity Management: Global Best Practices, Rothstein Publishing, 2014.
[32] Stéphane Hallegatte, Climate change impact on natural disaster losses, in: S. Hallegatte (Ed.), Natural Disasters and Climate Change: an Economic Perspective, Springer International Publishing, Cham, 2014, pp. 99–129.
[33] Nardia Haigh, The Natural Environment as a Primary Stakeholder: the Case of Climate Change - Haigh - 2009 - Business Strategy and the Environment, Wiley Online Library, 2007. October 31.
[34] Francesca Santucci, Martina Nobili, Luca Faramondi, Gabriele Oliva, Bianca Mazzà, Antonio Scala, Massimo Ciccozzi, Roberto Setola, Evaluating the COVID-19 impact in Italian regions via multi criteria analysis, PLoS One 18 (5) (2023) e0285452, https://doi.org/10.1371/journal.pone.0285452.
[35] J.K. Tay, W.S. Lim, W.S. Loh, K.S. Loh, Sustaining otolaryngology services for the long haul during the COVID-19 pandemic: experience from a tertiary health system, Otolaryngol. Head Neck Surg. 163 (1) (2020) 47–50, https://doi.org/10.1177/0194599820922983.
[36] M. Hennessey, B. Lee, T. Goldsmith, D. Halvorson, W. Hueston, K. McElroy, K. Waters, Supporting business continuity during a highly pathogenic Avian influenza outbreak: a collaboration of industry, academia, and government, Avian Dis. 54 (SUPPL. 1) (2010) 387–389, https://doi.org/10.1637/8700-031509-Reg.1.
[37] F. Gasbarro, F. Iraldo, T. Daddi, The drivers of multinational enterprises' climate change strategies: a quantitative study on climate-related risks and opportunities, J. Clean. Prod. 160 (2017) 8–26, https://doi.org/10.1016/j.jclepro.2017.03.018.
[38] Sooksan Kantabutra, Gayle C. Avery, Vision effects in customer and staff satisfaction: an empirical investigation, Leader. Organ. Dev. J. 28 (3) (2007) 209–229, https://doi.org/10.1108/01437730710739648.
[39] V. Vojtko, L. Rolínek, M. Plevný, System dynamics model of crises in small and medium enterprises, Economic Research-Ekonomska Istrazivanja 32 (1) (2019) 168–186, https://doi.org/10.1080/1331677X.2018.1552176.
[40] E. Sithirasenan, N. Almahdouri, Using WiMAX for effective business continuity during and after disaster, in: IWCMC 2010 - Proceedings of the 6th International Wireless Communications and Mobile Computing Conference, 2010, pp. 494–498. Caen.
[41] G.G. Hom, A.P. Chous, The prospect of pandemic influenza: why should the optometrist be concerned about a public health problem? Optometry 78 (12) (2007) 629–643, https://doi.org/10.1016/j.optm.2007.04.099.
[42] Francis Chateauraynaud, Alertes Et Lanceurs D'Alerte, Humensis, 2020.
[43] Nikola Marangunić, Andrina Granić, Technology acceptance model: a literature review from 1986 to 2013, Univers. Access Inf. Soc. 14 (1) (2015) 81–95, https://doi.org/10.1007/s10209-014-0348-1.
[44] B.R.M. Manning, Year 2000 and all that: securing business continuity, Eng. Sci. Educ. J. 8 (6) (1999) 243–248, https://doi.org/10.1049/esej:19990601.
[45] E.E. Bennett, R.R. McWhorter, Virtual hrd's role in crisis and the post Covid-19 professional lifeworld: accelerating skills for digital transformation, Adv. Develop. Hum. Resour. 23 (1) (2021) 5–25, https://doi.org/10.1177/1523422320973288.
[46] Elisabeth E. Bennett, Virtual HRD: the intersection of knowledge management, culture, and intranets, Adv. Develop. Hum. Resour. 11 (3) (2009) 362–374, https://doi.org/10.1177/1523422309339724.
[47] X. Bai Chen, Y. Zhu, H. Wei, Research on power dispatching automation system based on cloud computing, in: 2012 IEEE Innovative Smart Grid Technologies - Asia, ISGT Asia 2012, Tianjin, 2012.
[48] T. Kihara, D. Gichoya, Use of cloud computing platform for E-Learning in institutions of higher learning in Kenya, in: *2014 IST-Africa Conference and Exhibition, IST-Africa 2014*. Le Meridien Ile Maurice, IEEE Computer Society, 2014.
[49] K. Tang, Research on disaster recovery model of cloud-based digital library, Appl. Mech. Mater. 336–338 (2013) 2134–2137. https://dx.doi.org/10.4028/www.scientific.net/AMM.336-338.2134.
[50] J. Pingel, C. Case, B. Amer, R.A. Hornung, A.H. Schmidt, World marrow donor association crisis response, business continuity, and disaster recovery guidelines, Biol. Blood Marrow Transplant. 18 (12) (2012) 1785–1789, https://doi.org/10.1016/j.bbmt.2012.08.006.
[51] Larissa A. Grunig, James E. Grunig, William P. Ehling, What is an effective organization?, in: Excellence in Public Relations and Communication Management Routledge, 2008.
[52] F. Mongioi, L. McNally, R. Thompson, Integrating measures for business continuity and transportation demand management to ensure regional emergency preparedness and mobility, Transp. Res. Rec. (2137) (2009) 85–94, https://doi.org/10.3141/2137-10.
[53] G. Parise, L. Parise, L. Martirano, A. Germole, The relevance of the architecture of electrical power systems in hospitals: the service continuity safety by design, in: 2015 IEEE/IAS 51st Industrial and Commercial Power Systems Technical Conference, I and CPS 2015, Institute of Electrical and Electronics Engineers Inc, 2015.
[54] D.B. Dimov, Y. Tsonev, Semi-automated system updates deployment solution assuring zero business disruption, in: 2018 20th International Symposium on Electrical Apparatus and Technologies, SIELA 2018 - Proceedings, Institute of Electrical and Electronics Engineers Inc, 2018.
[55] M.L. Jensen, A. Durcikova, R.T. Wright, Using susceptibility claims to motivate behaviour change in IT security, Eur. J. Inf. Syst. (2019) 1–19, https://doi.org/10.1080/0960085X.2020.1793696.
[56] A.M. Heikkilä, R. Molarius, T. Uusitalo, Vulnerability of complex critical systems: case water supply and distribution networks, Int. J. Risk Assess. Manag. 15 (2–3) (2011) 241–257, https://doi.org/10.1504/IJRAM.2011.042119.
[57] Florian Jell, Theoretical foundations, in: F. Jell (Ed.), Patent Filing Strategies and Patent Management: an Empirical Study, Gabler Verlag, Wiesbaden, 2012, pp. 4–14.
[58] Mustafa Hashmi, Guido Governatori, Norms modeling constructs of business process compliance management frameworks: a conceptual evaluation, Artif. Intell. Law 26 (3) (2018) 251–305, https://doi.org/10.1007/s10506-017-9215-8.
[59] R. Al-Shaikh, Z. Al-Hussain, A. Al-Sharidah, Toward building an IT disaster recovery site for oil and gas companies, in: A.-D.D. Romanovs A, G. Merkuryeva, Y. Merkuryev (Eds.), Proceedings - 7th International Conference on Computational Intelligence, Communication Systems and Networks, CICSyN 2015, Institute of Electrical and Electronics Engineers Inc, 2015, pp. 169–173.
[60] J. Martin, Working and training from home, in: Proceedings ACM SIGUCCS User Services Conference, 2007, pp. 227–229.
[61] D. Achmadi, Y. Suryanto, K. Ramli, On developing information security management system (ISMS) framework for ISO 27001-Based data center, in: 2018 International Workshop on Big Data and Information Security, IWBIS 2018, Institute of Electrical and Electronics Engineers Inc, 2018, pp. 149–157.
[62] Anon, ISO/IEC 27001:2005 - information technology — security techniques — information security management systems — requirements, iTeh Standards Store (2015). September 30, 2022, https://standards.iteh.ai/catalog/standards/iso/edd8976e-8ad3-4d6d-b16a-824e1629eeab/iso-iec-27001-2005.

[63] Standards, European.n.d. “BS 25999-2:2007 (USA edition) business continuity management specification.” Https://Www.En-Standard.Eu. Retrieved September 30, 2022 (https://www.en-standard.eu/bs-25999-2-2007-usa-edition-business-continuity-management-specification/).
[64] W. Boehmer, Toward a target function of an information security management system, in: Proceedings - 10th IEEE International Conference on Computer and Information Technology, CIT-2010, 7th IEEE International Conference on Embedded Software and Systems, ICESS-2010, ScalCom-2010, 2010, pp. 809–816. Bradford.
[65] S. Karthik, S. Kenkre, K. Narayanam, V. Pandit, Recourse aware resource allocation for contingency planning in distributed service delivery, in: Proceedings of 2012 IEEE International Conference on Service Operations and Logistics, and Informatics, SOLI 2012, Suzhou, 2012, pp. 48–53.
[66] Ralph Johnson, Brian Foote, Designing reusable classes, J. Object-Oriented Program. 1 (1988), 22textendash35.
[67] Han Albrecht Schmid, Systematic framework design by generalization, Commun. ACM 40 (10) (1997) 48–51, https://doi.org/10.1145/262793.262803.
[68] F. Faisal, The backup recovery strategy selection to maintain the business continuity plan, in: H.A. Comfort L, R. Haigh, F.A. Ismail (Eds.), MATEC Web of Conferences, vol. 229, EDP Sciences, 2018.
[69] S. Papagiannidis, J. Harris, D. Morton, WHO led the digital transformation of your company? A reflection of IT related challenges during the pandemic, Int. J. Inf. Manag. 55 (2020), https://doi.org/10.1016/j.ijinfomgt.2020.102166.
[70] M.S. Al-Qahtani, H.M. Farooq, Securing a large-scale data center using a multi-core enclave model, in: Proceedings - UKSim-AMSS 11th European Modelling Symposium on Computer Modelling and Simulation, EMS 2017, Institute of Electrical and Electronics Engineers Inc, 2017, pp. 221–226.
[71] Evan Heit, The instantiation principle in natural categories, Memory 4 (4) (1996) 413–452, https://doi.org/10.1080/096582196388915.
[72] X. Xiong, X. Jia, P. Liu, SHELF: preserving business continuity and availability in an intrusion recovery system, in: Proceedings - Annual Computer Security Applications Conference, ACSAC, Honolulu, HI, 2009, pp. 484–493.
[73] Don Vandewalle, Development and validation of a work domain goal orientation instrument, Educ. Psychol. Meas. 57 (6) (1997) 995–1015, https://doi.org/10.1177/0013164497057006009.
[74] X.C. Yin, Z.G. Liu, L. Nkenyereye, B. Ndibanje, Toward an applied cyber security solution in iot-based smart grids: an intrusion detection system approach, Sensors (Switzerland) 19 (22) (2019), https://doi.org/10.3390/s19224952.
[75] B. Pranggono, J.M.H. Elmirghani, Traffic statistics in WDM storage area networks, in: Proceedings of 2008 10th Anniversary International Conference on Transparent Optical Networks, vol. 3, ICTON, Athens, 2008, pp. 89–92.
[76] S. Malladi, J.T. Weaver, T. Goldsmith, W. Hueston, S. Voss, J. Funk, C. Der, K.E. Bjork, T.L. Clouse, M. Hennessey, F. Sampedro, B. Lee, D.A. Halvorson, The impact of holding time on the likelihood of moving internally contaminated eggs from a highly pathogenic avian influenza infected but undetected commercial table-egg layer flock, Avian Dis. 56 (4 SUPPL.1) (2012) 897–904, https://doi.org/10.1637/10191-041012-Reg.1.
[77] P. Deshanta Ibnugraha, L.E. Nugroho, P.I. Santosa, Metrics analysis of risk profile: a perspective on business aspects, in: *2018 International Conference on Information and Communications Technology, ICOIACT 2018*. Vols. 2018-January, Institute of Electrical and Electronics Engineers Inc, 2018, pp. 275–279.
[78] P. Wilkinson, J. Glockling, D. Bouchlaghem, K. Ruikar, Using business impact analyses to enhance resilient fire engineering building design, Architect. Eng. Des. Manag. 9 (4) (2013) 229–249, https://doi.org/10.1080/17452007.2012.738043.
[79] J.W. Liu, Using big data database to construct new GFuzzy text mining and decision algorithm for targeting and classifying customers, Comput. Ind. Eng. 128 (2019) 1088–1095, https://doi.org/10.1016/j.cie.2018.04.003.
[80] R. Sandhu, R. Krishnan, G.B. White, Towards secure information sharing models for community cyber security, in: Proceedings of the 6th International Conference on Collaborative Computing: Networking, Applications and Worksharing, CollaborateCom 2010, IEEE Computer Society, 2010.
[81] Maximilian Röglinger, Jens Pöppelbuß, Jörg Becker, Maturity models in business process management, Bus. Process Manag. J. 18 (2) (2012) 328–346, https://doi.org/10.1108/14637151211225225.
[82] D.L. King, Moving towards a business continuity culture, Netw. Secur. 2003 (1) (2003) 12–17, https://doi.org/10.1016/S1353-4858(03)00112-0.
[83] M.A. Al-Khalifa, The talent gap in the E&P industry: causes and recommended solutions, in: Society of Petroleum Engineers - Abu Dhabi International Petroleum Exhibition and Conference 2016, Society of Petroleum Engineers, 2016. Vols. 2016-January.
[84] Jonah Kowall, Will Cappelli, Magic Quadrant for Application Performance Monitoring, vol. 28, 2012.
[85] Y. Song, R. Routray, Y. Hou, Scalable data analytics platform for enterprise backup management, in: IEEE/IFIP NOMS 2014 - IEEE/IFIP Network Operations and Management Symposium: Management in a Software Defined World, IEEE Computer Society, Krakow, 2014.
[86] Mariam Ben Hassen, Turki Mohamed, Gargouri Faïez, Choosing a sensitive business process modeling formalism for knowledge identification, Procedia Comput. Sci. 100 (2016) 1002–1015, https://doi.org/10.1016/j.procs.2016.09.272.
[87] D. Draheim, R. Pirinen, Towards exploiting social software for business continuity management, in: Proceedings - International Workshop on Database and Expert Systems Applications, DEXA, Toulouse, 2011, pp. 279–283.
[88] Yu Cui, Hiroki Idota, Masaharu Ota, Improving supply chain resilience with implementation of new system architecture, in: 2019 IEEE Social Implications of Technology (SIT) and Information Management (SITIM), 2019, pp. 1–6.
[89] Y. Wang, U. Iqbal, Y. Gong, The performance of resilient supply chain sustainability in COVID-19 by sourcing technological integration, Sustainability 13 (11) (2021), https://doi.org/10.3390/su13116151.
[90] Valentas Gružauskas, Mantas Vilkas, Managing capabilities for supply chain resilience through it integration, Economics and Business 31 (1) (2017) 30–43, https://doi.org/10.1515/eb-2017-0016.
[91] L. Chunsheng, C.W.Y. Wong, C.C. Yang, K.C. Shang, T.C. Lirn, Value of supply chain resilience: roles of culture, flexibility, and integration, Int. J. Phys. Distrib. Logist. Manag. 50 (1) (2020) 80–100, https://doi.org/10.1108/IJPDLM-02-2019-0041.
[92] V. Hristidis, S.C. Chen, T. Li, S. Luis, Y. Deng, Survey of data management and analysis in disaster situations, J. Syst. Software 83 (10) (2010) 1701–1714, https://doi.org/10.1016/j.jss.2010.04.065.
[93] R. Power, D. Forte, You don’t need a weatherman to know which way the wind blows: business continuity in the 21st century, in: *Computer Fraud and Security* 2006, 2006, pp. 17–19, https://doi.org/10.1016/S1361-3723(06)70411-0, 8.
[94] A. Kolah, B. Foss, M. Hickley, What should UK and US marketers Do to prepare for the biggest threat to business continuity for a decade? J. Direct, Data Digital Mark. Pract. 17 (2) (2015) 86–92, https://doi.org/10.1057/dddmp.2015.50.
[95] H.S. Al-Hashem, H.A. Al-Essa, Towards data availability solutions during disaster, in: H.-A. Y (Ed.), 6th International Conference on Information and Communication Technologies for Disaster Management, ICT-DM 2019, Institute of Electrical and Electronics Engineers Inc, 2019.
[96] Robert L. Linn, Eva L. Baker, Stephen B. Dunbar, Complex, performance-based assessment: expectations and validation criteria, Educ. Res. 20 (8) (1991) 15–21, https://doi.org/10.3102/0013189X020008015.
[97] M. Pero, I. Sudy, Increasing security and efficiency in supply chains: a five-step approach, Int. J. Shipp. Transp. Logist. (IJSTL) 6 (3) (2014) 257–279, https://doi.org/10.1504/IJSTL.2014.060785.