International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Exploring Information Systems for Business Continuity Planning in IT-Driven Organizations Post-Pandemic: Insight into Enhancing Future Resilience

Sunish Vengathattil

Wilmington University

Abstract

Business continuity management provides holistic and proactive approaches for businesses to effectively manage the potential disruption caused by unforeseen events. Despite the benefits, most organizations are reluctant to adopt effective systems for BCP due to implementation technicalities, complacency, lack of tools and resources, and lack of training. This explorative study leverages case studies to examine and critically analyze how information systems can be leveraged to create, test, execute, and maintain BCPs in IT-driven companies. The case studies focus on the information systems leveraged by a purposively selected sample of Fortune 500 companies. The chosen companies include Walmart, Amazon, Apple, Microsoft, Toyota, General Motors, and IBM. The diversity and credibility of the findings are enhanced by incorporating systems used by a selected sample of large IT-driven companies not listed in the Fortune 500 list. The recommended strategies for using systems to reduce the cost of BCP include adopting cloud-based solutions, automation, virtualization, risk assessment, and standardization. The recommendations to educate organizations on the risks of operating without robust BCPs include awareness campaigns, real-world case studies, compliance requirements, and financial incentives. Implementing the proposed strategies enables organizations to leverage cost-effective, scalable, and reliable information systems to automate BCPs and operations, enhancing competitiveness and resilience to disruptions.

Introduction

Background

Business continuity planning is creating systems of prevention and recovery to deal with potential threats to a company. Building a Business Continuity Plan (BCP) helps organizations prepare for unexpected events such as natural disasters, cyber-attacks, and pandemics, which could negatively impact their operations (McCrackan, 2004). One of the main benefits of having a BCP is that it helps organizations minimize the impact of a disruptive event. BCP is vital for companies that provide critical services such as healthcare, finance, and utilities, where downtime can significantly affect the company and its customers. Another crucial aspect of a BCP is that it helps organizations to maintain their reputation and credibility in the market. A well-designed BCP can demonstrate to customers and stakeholders that the organization is committed to providing reliable and continuous services, even in adversity. A BCP is also necessary for organizations to comply with industry regulations (ISO, 2019). Many industries, such as finance and healthcare, have specific rules that require organizations to have a BCP in place (Federal

Reserve Board, 2017; Yale University, 2019).

The COVID-19 pandemic inspired companies to develop and deploy innovative solutions and strategies to address supply chain disruptions and customer needs and preferences changes. Corporate executives learned the significance of preparedness to effectively respond to unforeseen disasters to ensure business continuity and sustainability (Margherita & Heikkilä, 2021). Business Continuity Management (BCM) has advanced from the 1970s into a robust strategy for responding to technical, operational, and risk-related interruptions to guarantee continuity and protect diverse stakeholders' interests. According to Corrales-Estrada et al. (2021), BCM is a comprehensive management approach that recognizes potential threats to an organization and the future effects on business operations. BCM provides a dynamic structure for developing organizational resilience with the capacity to respond effectively to protect key stakeholders' value-adding operations, brand, and interests.

A study by Margherita and Heikkilä (2021) revealed that of the 50 Fortune 500 companies surveyed, a majority had inadequate business continuity plans (BCPs) and were consequently unable to respond to challenges exacerbated by the pandemic sufficiently. Toyota, for instance, was forced to reduce its production owing to an overlooked need for BCPs (Margherita & Heikkilä, 2021). Conversely, with well-maintained and effectively managed BCPs, organizations such as BP could continue operations and provide a steady fuel supply to customers. Margherita and Heikkilä (2021) discovered that a tiny percentage of companies could maintain viable business continuity during the pandemic. This study aims to analyze the cause of this phenomenon and develop strategies to equip more businesses to survive similar future interruptions, helping meet society's fundamental economic and social needs.

Problem Statement

The main problem we face in this area is that, despite the numerous benefits of having a Business Continuity Plan (BCP), many companies are still reluctant to invest in this critical aspect of risk management (Zeng & Zio, 2017). There are many reasons for this behavior. 1) Lack of awareness - Some companies are unaware of the importance of having a BCP. They may not understand the potential consequences of not having a plan, such as financial losses, customer dissatisfaction, and damage to their reputation. 2) Perceived cost - Developing and implementing a BCP can be expensive and time-consuming. Investing in a BCP may not be a priority for companies struggling with tight budgets. 3) Complacency - Some companies believe that they will never face a situation that would require the use of a BCP. They may see it as an unnecessary expense and a low priority, especially if they have never experienced a significant interruption in their operations. 4) Lack of ownership - BCPs often fall between departments and individuals, with no one taking full responsibility for ensuring its implementation and maintenance. This results in a lack of action and investment. 5) Inadequate resources - Companies with limited resources, such as small businesses or startups, may find it challenging to allocate the necessary personnel and financial resources to develop and implement a BCP. 5) Resistance to change - Some companies may resist change. Implementing a BCP may require significant changes to their current processes and systems, creating resistance and reluctance to invest in it (Zeng & Zio, 2017). However, it is essential to remember that the benefits of having a BCP far outweigh the costs. It helps organizations respond quickly and effectively to interruptions, minimize the impact of downtime, and maintain their competitive edge (Tammineedi, 2010). Overall, Business Continuity Plans (BCPs) must be a part of the fundamental operational process of all Fortune 500 companies. However, despite all the recommendations on industrial best practices, most of our Fortune 500 companies lack adequate BCPs. If these organizations fail to

implement the best practices in BCPs, they must imbibe significant losses during the next impacting natural calamity or a pandemic.

The COVID-19 pandemic had adverse implications on economies worldwide, with global economic activity estimated to have declined by 3.2%, trade plummeting by 5.3%, and the US GDP reduced by 3.4% in 2020 (Chang et al., 2022, p.2). Although the economic impacts are massive, their human cost is even more devastating when assessed using population health metrics such as disability-adjusted life years (DALYs). The effect of COVID-19 in 2020 alone is greater than that of all epidemics and disasters over the last two decades. Due to the rapid deployment of technology in various sectors, systems, particularly those associated with critical infrastructures in process industries, are becoming more vulnerable to the potential for disruption from multiple sources, including unexpected system breakdowns, natural catastrophes, cyber-attacks, and terrorist attacks (Zeng & Zio, 2017).

Margherita and Heikkilä (2021) study revealed that a select few Fortune 500 companies could maintain adequate business continuity during the pandemic. Despite the increasing value of business continuity planning during pandemics and disasters, there is a lack of comprehensive research on the role of information systems in creating, testing, maintaining, and executing business continuity plans in digitally powered companies. Likewise, current research lacks robust frameworks for guiding the effective use of systems in ensuring business continuity and resilience during crises. Consequently, this study will explore the prevalent problems and propose solutions for effectively leveraging information systems to create, test, maintain, and execute business continuity plans in IT-driven companies.

Purpose

This research aims to comprehensively investigate and analyze the role of information systems in creating, testing, maintaining, and executing business continuity in IT-driven companies. The research seeks to identify best practices and formulate a framework for effective information system utilization to bolster resilience and rapid recovery from disruption caused by unforeseen events and disasters. As a result, it will enable and empower organizations to overcome cost barriers and soothe the impact of the scarcity of resources (McCrackan. 2004). In addition to cost efficiency, this research proposes an effective awareness program to make medium-to-large-scale organizations aware of the benefits of maintaining BCPs and the risks of not having them. A measurable risk, in terms of cost and probability of a qualifying event, will help educate the organizational leadership to adopt the recommendations on BCPs. The risk assessment and a cost-efficient solution will lure most Fortune 500 companies to invest in BCPs (Margherita & Heikkilä, 2021). With the two outlined purposes in mind, we may define the research questions explained below, answering which will serve the purpose of this research.

Research Questions and Objectives

Main Questions

The primary questions this study is seeking to answer are:

- RQ1: How can Information Systems be used to make the cost of BCPs affordable to most large-scale Fortune 500 companies?
- RQ2: What can be done to educate large-scale organizations on the cost of risk that they are taking by proceeding without adequate BCPs in place?

Sub-Questions

This research will also chase answers to the following sub-questions.

- RSQ1: How do information systems support the creation and execution of business continuity plans in IT-driven companies in the context of the COVID-19 pandemic?
- RSQ2: What is the interrelationship between business continuity management, risk management, crisis management, and disaster recovery in a digitally powered environment?
- RSQ3: What challenges are IT-driven companies facing in deploying and executing business continuity and disaster recovery plans?
- RSQ4: How can a framework be developed to guide the effective use of systems in creating, testing, maintaining, and executing BCPs in digitally powered companies during a crisis or disaster?
- RSQ5: What are the best practices and solutions for empowering IT-driven organizations to leverage business continuity and disaster recovery to increase resilience and sustainability against unforeseen events?

Objectives

- To analyze how information systems can help IT-driven companies develop and deploy business continuity plans post-pandemic.
- To explore the interrelationship between business continuity management, risk management, crisis management, and disaster recovery in a digitally powered environment.
- To examine IT-driven companies' challenges in deploying and executing business continuity and disaster recovery plans.
- To develop a framework to guide the effective use of systems in creating, testing, maintaining, and executing BCPs in IT-driven companies during a crisis or disaster.
- To identify best practices and solutions for empowering digitally powered organizations to leverage business continuity and disaster recovery to increase resilience and sustainability against unforeseen events.

Proposition

The COVID-19 pandemic has exposed significant gaps in the ability of organizations to respond to and manage crises, particularly in business continuity planning (Margherita & Heikkilä, 2021). Organizations are increasingly cognizant of the significance of Business Continuity Management (BCM). BCM aims to guarantee consistent access to all crucial business resources necessary to facilitate critical business processes during business disruption while hastening the transition back to a functioning "business as usual" (Tammineedi, 2010). The rationale for this study is to empower organizations to increase their resistance and resilience to disruptions caused by unforeseen events using information systems to create, test, maintain, and execute business continuity plans. By utilizing information systems in business continuity planning and disaster recovery, IT-driven companies can successfully plan, strategize, and manage unforeseen events, ultimately leading to increased organizational resilience.

Similarly, the study presents an in-depth investigation into the use of information systems to create, test, maintain, and execute business continuity plans, exploring its theoretical and practical implications. The study focuses on developing frameworks and strategies to enable organizations to manage the effects of disruptions better and the best practices for creating, testing, maintaining, and executing business continuity and disaster recovery plans. Besides, the study examines the impact of systems on organizational resilience and how organizations can effectively utilize them to prepare and respond to disruptions. The results provide valuable insights into how IT-driven companies can effectively use

systems to increase their resilience to disruptions caused by unforeseen events, including pandemics, technological disruptions, and natural hazards.

Definitions

The following definitions are used throughout this research paper with the context as explained below.

- Business Continuity Plan (BCP): A Business Continuity Plan (BCP) is a comprehensive strategy that outlines how an organization will continue to operate during and after a disruptive event. The purpose of a BCP is to minimize the impact of disruptions to critical business functions and processes, ensure the safety of employees, and protect against loss of data, revenue, and reputation. The BCP includes steps for incident response, disaster recovery, and preserving critical business functions. It should be regularly reviewed and updated for organizational changes, technology, and risks. The BCP is a vital component of an organization's risk management program, helping to ensure that the business can quickly recover from unexpected events (Campbell & Brown, 2015).
- Business Continuity Management (BCM): Business Continuity Management (BCM) is a holistic and proactive approach to managing potential disruptions to an organization's operations. It involves identifying critical business functions and processes, assessing potential risks, and developing and implementing plans to minimize the impact of disruptions. BCM also involves ongoing monitoring, testing, and review of business continuity plans to ensure they remain practical and updated. BCM aims to ensure that an organization can quickly and effectively respond to disruptions, maintain critical business functions, and minimize the impact on customers, employees, and stakeholders. BCM is an essential component of an organization's overall risk management strategy, helping to protect against loss of revenue, data, and reputation (Tammineedi, 2010).
- IT-Driven Organizations: IT-driven organizations are companies where information technology (IT) plays a central role in all aspects of the business, including decision-making, operations, and strategy. In these organizations, technology is leveraged to streamline processes, automate tasks, improve communication and collaboration, and enhance the customer experience. IT-driven organizations often rely heavily on data and analytics to inform their business decisions, and their success is closely tied to their ability to utilize and manage technology effectively. IT is not just a support function in these organizations but a vital business enabler. It requires a strong alignment between IT and business goals and a culture that values technology and innovation. The effective use of technology is crucial for the success of IT-driven organizations in today's digital business environment (Campbell & Brown, 2015).

Literature Review

Introduction

Overview

This chapter presents a comprehensive evaluation and critical analysis of the relevant literature on the topic of the study. This review aims to analyze the current body of knowledge on the subject, structure it so the reader can easily interpret it, and serve as the foundation for the research questions and objectives. The researcher gains a better understanding of the context and scope of the topic by critically analyzing and evaluating updated peer-reviewed literature. The comprehensive review is structured around the research topic and questions covering established and emerging knowledge. An in-depth summary of each source's main findings and contribution to the field is presented and synthesized. Besides, gaps and areas

for further research to maximize information systems in creating, testing, maintaining, and executing BCP plans in IT-driven companies beyond the pandemic are highlighted.

Business Continuity Planning (BCP) is an essential element in any IT-driven company, as it provides a way to ensure continuity of operations following a disruption. Creating, testing, and maintaining BCP plans is critical for successful implementation. The study examines diverse research on using systems to develop, test, and maintain BCP plans in IT-driven companies. The review suggests that using information systems can be beneficial for creating, testing, and maintaining BCP plans. Business Continuity Management (BCM) software can help organizations develop and sustain their BCP plans by providing risk management, document management, and testing tools. Case studies of industry-leading solutions such as Microsoft Azure and Oracle Public Cloud will offer comprehensive and practical insights regarding the significance of business continuity planning and disaster recovery in a digitally powered environment.

Background

The study reviews extensive and diversified literature focusing on using information systems to support the creation, testing, maintenance, and execution of business continuity plans in IT-driven companies. The focus is to critically analyze updated literature, including top-notch solutions currently in the market and the best practices for testing business continuity plans, understanding the challenges IT-driven companies face in executing business continuity plans during the pandemic and developing a robust framework.

The review concentrates on case studies, experiments, and recently published sources examining information systems' design, development, and implementation concerning business continuity planning and disaster recovery. Besides, current theoretical frameworks and models that support the use of information systems in business continuity and disaster recovery are explored. Studies that detail the challenges and best practices associated with creating, testing, maintaining, and executing business continuity and disaster recovery plans in IT-driven companies are critically analyzed and evaluated.

Literature Search

The search strategy used to locate relevant research material for this study consisted of two steps.

Step 1: Keyword Search

The first step was to identify keywords relevant to the topic of the study. In this case, the search terms used were "information systems," "business continuity plans," "COVID-19 pandemic," and "IT-driven companies." The sources were retrieved from the University library and reputable online academic databases such as Google Scholar, Science Direct, Library Genesis, Emerald, Research Gate, NCBI, MDPI, and Open Access.

Step 2: Database Search

The second step of the search strategy was to search for relevant material in the academic databases listed above. The search terms identified in Step 1 were then used in combination with other keywords, such as "role," "create," "test," "maintain," and "execute," to narrow down the search results further.

In addition, advanced search filters were used to narrow down the results to peer-reviewed material published within the last ten years. The search results were then carefully reviewed for relevance to the study topic.

Business Continuity Management (BCM)

Business Continuity

The significance of Business Continuity Management (BCM) to organizational activities has been steadily increasing. The promulgation of ISO 22301 exemplifies this: Societal Security – Business Continuity Management Systems – Requirements, which serves as a testament to the recognition of BCM in achieving corporate success and ensuring service delivery availability. ISO 22301 has been a benchmark since its inception in 2012 for implementing and maintaining an efficient business continuity management system (BCMS) (ISO, 2019). While the specifications are accompanied by ISO 22313, which offers valuable insight into the fundamentals of the requirements, it does not provide all the details necessary to form the key processes.

ISO released the updated version of ISO 22301 in October 2019. ISO 22301:2019 is the most recent international standard for organizations to use to guarantee the continuity of operations during disruptive events (Leal, 2019). This updated version has superseded the 2012 standard. ISO 22301 requirements are intended to be comprehensive and applicable to all organizations, regardless of their size, type, and purpose (ISO, 2022). The extent of application of these requirements will depend on the complexity and circumstances of the organization.

Figure 1

History of the ISO 22301 Standard

(Adopted from Leal, 2019)

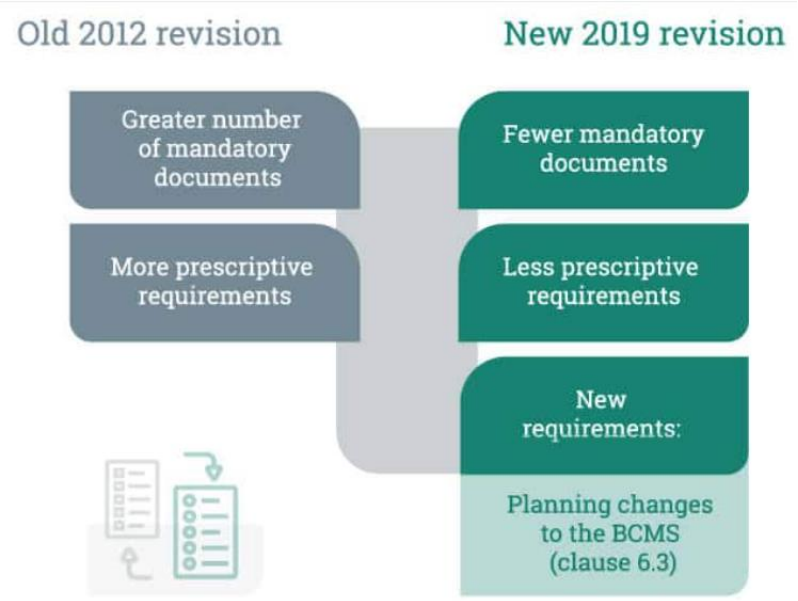
Note. Figure 1 presents a high-level summary of the history of the ISO 22301 standard.

The first publication in 2012 was based on BS 25999-2, and the current version was published in 2019. The most recent version of ISO 22301 is suitable for any organization of any size that is looking to establish, maintain, and improve a Business Continuity Management System (BCMS) to adhere to its stated business continuity policy, maintain an acceptable level of service during an interruption, and better their resilience through an effective BCMS (ISO, 2022).

The rapid pace of technological advancements, new regulations, increased competition, and customer demands have created an environment where businesses must evolve continually to succeed. Organizations must focus on time, quality, and compliance goals, and they must recognize that while some of these can create opportunities, others can have damaging effects if not appropriately managed (Wong & Shi, 2015, p.5). Business continuity management (BCM) is a proactive strategy that seeks to maximize

business potential. BCM is a field that combines management and technological aspects to protect companies' financial performance. Hence, it helps ensure operational continuity by mitigating the potential hazards and their associated impacts on essential business processes.

Figure 2



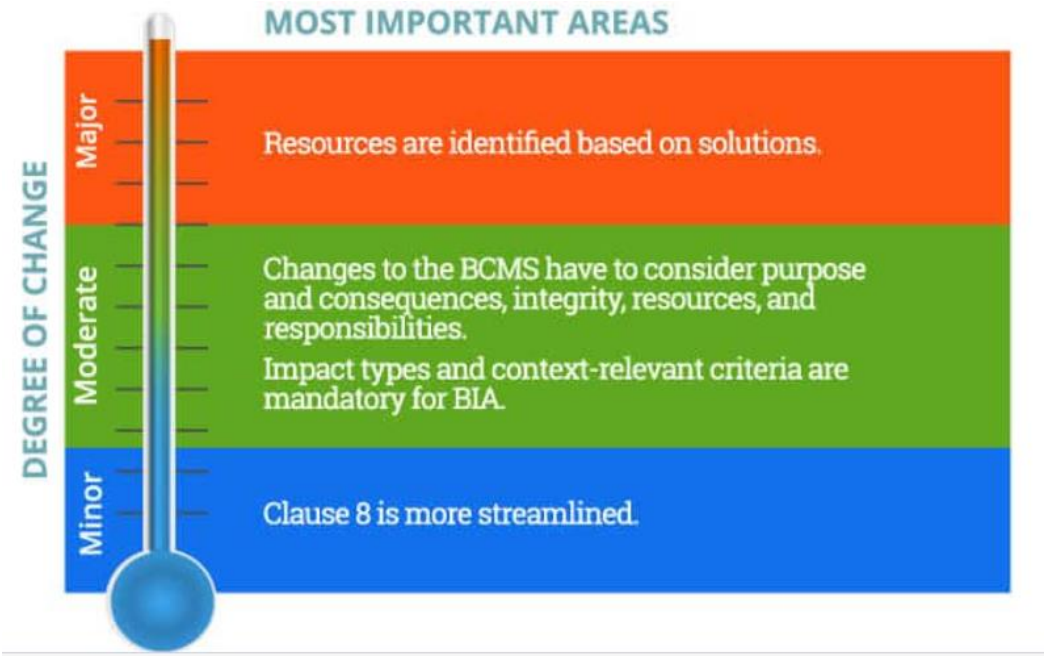
ISO 22301:2012 vs. 2019
(Adopted from Leal, 2019)

Note. Figure 2 highlights the main differences between the old and new ISO 22301. The latest version has fewer mandatory documents and prescriptive requirements. The 2019 version also has a novel condition for planning changes to the BCMS (Clause 6.3).

BCM is a comprehensive approach to ensuring the ongoing viability of an organization by identifying and preparing for potential threats that could disrupt operations. BCM creates organizational resilience to protect stakeholders' interests, maintain a positive reputation, and sustain the activities that generate value. BCM stands out by incorporating methodologies from various management aspects, including risk, strategy, finance, and project management (Wong & Shi, 2015, p.6). Therefore, it provides a comprehensive means of protecting an organization's critical assets.

The fundamental purpose of Business Continuity Management (BCM) is to ensure the sustainability of business operations in the event of an incident by maintaining performance and reducing adverse effects. To ensure the successful implementation of BCM, organizations should consider its core principles: a long-term focus, executive management support, governance, adherence to good business practices, involvement of multiple disciplines, effective communication, value preservation, and flexibility in response (Wong & Shi, 2015, p.7).

Figure 3



Degree of Change in ISO 22301;2019
(Adopted from Leal, 2019)

Note. Figure 3 highlights the extent of change in the most critical areas covered by ISO 22301, 2019.
Leal (2019) asserts that the impact types and context-relevant criteria are mandatory for BIA. The significant difference is that resources are identified based on solutions. A moderate change is that the BCMS must consider the purpose and consequences, integrity, resources, and responsibilities. The minor change is that Clause 8 is more streamlined in the new version.

BCM can be implemented in various ways, strategically and operationally. However, due to competition, legal requirements, and customer expectations, BCM is increasingly becoming a priority for top-level executives. The pandemic tested the resilience of business continuity plans and disaster recovery strategies implemented in various sectors. Acciarini, Boccardelli, & Vitale (2021) combined a case study approach with semi-structured interviews to explore how big companies in Italy responded to the challenges exacerbated by the pandemic and guaranteed business continuity. The findings of Acciarini, Boccardelli, & Vitale (2021) are relevant to this study because the semi-structured interviews mainly targeted CEOs of IT-driven companies, including mobile communications, media, and banking sectors.

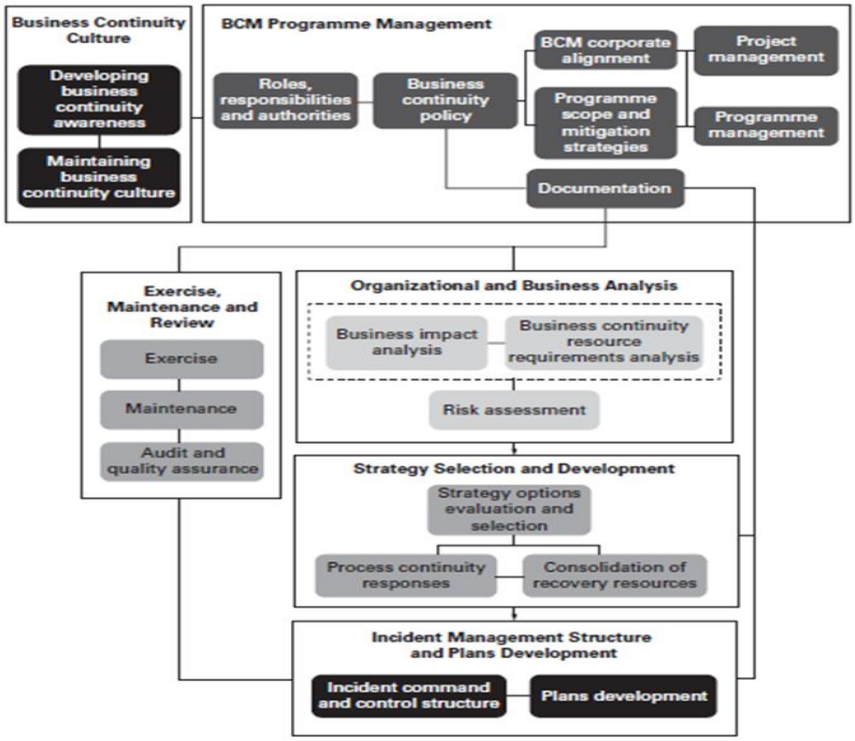
An examination of existing research has revealed that numerous applications of new technologies are being explored regarding their potential to assist with the COVID-19 pandemic (Frank et al., 2019; Ishack & Lipner, 2020; Kumar et al., 2020a, as cited by Acciarini, Boccardelli, & Vitale, 2021). For example, Frank et al. (2019) and Kumar et al. (2020) highlighted the advantages of digital solutions for medical care, treatment, and follow-up and to improve service delivery in retail contexts (Acciarini, Boccardelli, & Vitale, 2021).

Despite the benefits of BCM, extensive research has revealed various issues and gaps that need to be addressed. According to Acciarini, Boccardelli, & Vitale (2021), future research can analyze if the collaboration between commercial and institutional entities can take advantage of potential benefits in unforeseen circumstances. Specifically, the function of institutional proximity can be studied to determine if firms with comparable institutional structures tend to answer similarly to crises (Acciarini, Boccardelli,

& Vitale, 2021, p.347). For example, does forming strategic partnerships increase the probability of organizational resilience? In this case, comparative studies employing various industries and institutional frameworks can offer fruitful information.

The business continuity management lifecycle is a continuous and cyclical process. This model is based on the most common approaches taken in the BCM field and is broken into six components that are related to one another: BCM Programme management, organizational and business analysis, strategy selection and development, incident management structure and plans development, exercise, maintenance, and review, and a business continuity culture (Wong & Shi, 2015, p.12).

Figure 4



Business Continuity Management Lifecycle

(Adopted from Wong & Shi, 2015, p.24)

Note. Figure 4 shows a comprehensive overview of the business continuity management lifecycle components.

The Need for Business Continuity Planning

Business continuity is an organization's ability to maintain its operations, including delivering its products and services, within acceptable timeframes and at predefined capacities, despite disruptions or disasters (ISO, 2019). A Business Continuity Plan is a comprehensive document that outlines how an organization will respond to and recover from a disaster. More so, it describes the strategies, processes, and procedures necessary to ensure the delivery of products and services is resumed, recovered, and restored to meet business continuity objectives (ISO, 2019).

According to Mukherjee et al. (2020), the COVID-19 pandemic is a possible catalyst for economic expansion and sustaining livelihoods while preserving the environment and bettering the welfare of the populace through a model of Ecosystem-centric Business Continuity Planning. A 'Business Continuity

Plan' (BCP) strives to prepare organizations to remain in operation during a disruption by providing control and capabilities and preserving their strategic objectives and principles (Mukherjee et al., 2020). Besides, it should ensure that the company meets safe industrial standards for prosperity and emission for increased sustainability and resilience. Secondary research was employed to build the conceptual outline and principles of the 'Eco-centric BCP.'

Chang et al. (2022) investigated how companies responded to the COVID-19 pandemic compared to other disasters. The findings show that the pandemic's consequences echo those of prior disasters. Smaller companies, those susceptible to supply chain interruptions, those dealing with disrupted markets, and local businesses in areas hit the hardest all experience more incredible difficulty recovering (Chang et al., 2022). Firms often face difficulty replenishing their supplies due to the damage that disasters can cause to production sites, resulting in a decreased output of the goods and services necessary for other businesses to operate (Chang et al., 2022, p.6). These shortages can stretch across local and distant areas, significantly impacting recovery. The speed and flexibility of the disaster aid provided are critical to the successful revival of business operations. As a result, all these parameters must be considered when developing and implementing BCP and recovery plans in an IT-driven organization.

Information Systems for Business Continuity Management

An effective management system is a cyclical approach streamlining an organization's activities by systemizing its overall structure, planning processes, responsibilities, and resources. The system allows the organization to develop its strategy, transform it into actionable items, and monitor and improve the effectiveness of its management capability (Wong & Shi, 2015, p.28). Given its general applicability, executives must establish the objectives and activities tailored to suit the organization's particular needs when implementing the system.

An effective management system consists of a set of interconnected components which work together to create policies, set objectives, and develop processes to achieve them. The components include the organization's structure, roles, responsibilities, strategies, and plans for operations (ISO, 2019). By establishing a unified and organized plan for the organization, a management system helps to ensure that goals are achieved and that the organization runs efficiently (ISO, 2019). A management system can be tailored to address the needs of a single discipline or multiple disciplines.

Figure 5

Level	Objective	Activity/Assessment
1	Develop an **awareness** of the subject	• Introduce the concepts of the standard in the management processes. • The assessment is in the form of internal audits (also known as first-party audits) that are conducted by the organization for management review and other internal purposes.

2	Establish a **compliance culture** of the standard	• Develop and incorporate an ongoing management framework (based on the specified principles of the standard) in the management processes. • The assessment is conducted by parties having an interest in the organization, such as clients, or by agents engaged on their behalf. This is called supplier audit, also known as second-party audit.
3	Achieve a **certification** of the management system	• Establish a policy, objectives and a series of activities (in accordance to the requirements of the standard) in the management processes. • The assessment is conducted by independent auditing organizations or those providing certification. This is also called the third-party audit.

Levels of Management System Application

(Adopted from Wong & Shi, 2015, p.30)

Note. Figure 5 shows the levels of management system application.

The International Standardization Organization (ISO) 22301 is the world's first international standard for Business Continuity Management (BCM). This publication signifies the developing agreement of BCM's capacity to enhance organizational effectiveness. ISO 22301 consolidates all existing standards and best practices to generate an all-encompassing approach to BCM. The aim is to create a BCMS tailored to the organization's needs and capable of responding appropriately to disruptions, thus limiting their detrimental effects (Wong & Shi, 2015, p.31). Nevertheless, proper leadership and enough resources to be allocated to manage the BCMS are essential for this to be effective.

The Business Continuity Management System (BCMS) is an essential tool for organizations to ensure that their operations remain resilient in the face of disruptions. BCMS involves establishing policies and processes for the organization to ensure its vital functions are maintained and continued in the face of interruption. The BCMS includes the following key components: a business continuity policy, clearly defined roles and responsibilities, management processes for the BCMS, documentation, and other relevant BCM processes.

Galbusera, Cardarilli, & Giannopoulos (2021) critically analyzed the findings of the "*COVID-19: Emergency & Business Continuity*" survey by the European Commission's Joint Research Centre. The survey, conducted in April-May 2020, involved critical infrastructure experts, industry representatives, and relevant stakeholders. The findings reveal the various ways different companies responded to the challenges of the pandemic and ensured business continuity.

For instance, question 6 of the survey stated: *To the best of your knowledge, was your organization's core business negatively affected by the COVID-19 emergency so far?*" (Galbusera, Cardarilli, & Giannopoulos, 2021, p.4). Question 13 stated: "*Does your organization have a Business Continuity Plan to face an*

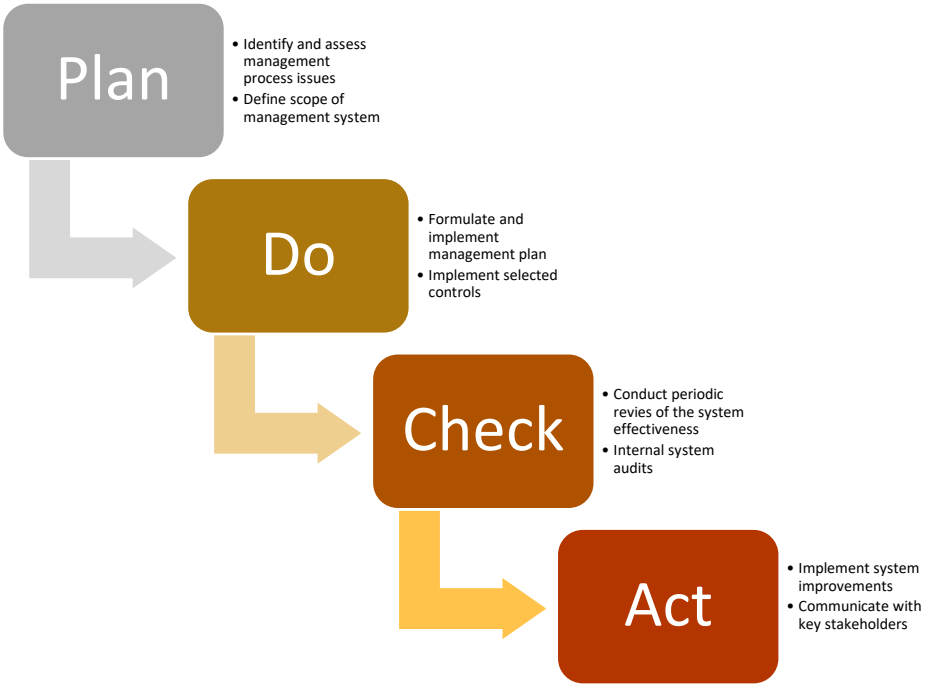
emergency?" (Galbusera, Cardarilli, & Giannopoulos, 2021, p.6). Most survey respondents stated that their organization (53.39%) or individual departments/functions (29.66%) have an implemented Business Continuity Plan, whereas 11.86% specified that it does not exist, and the rest chose not to answer. By incorporating the data from Question 3, public authorities (64.29%) and essential service industries or operators (53.85%) generally have organization-level BCPs in place. In comparison, universities and research institutes (34.62%) have lesser adoption of these plans, and consultancies (16.67%) have the least (Galbusera, Cardarilli, & Giannopoulos, 2021).

The Plan-Do-Check-Act (PDCA) Paradigm

At the core of ISO 22301 lies the Plan-Do-Check-Act (PDCA) cycle, which is the driving force that optimizes the operations of the Business Continuity Management System. This cycle is essential to any management system and ensures that organizations can fully complete the management system cycle to accomplish the desired objectives.

Figure 6

PDCA Paradigm



Note. Figure 6 shows the critical components of the PDCA paradigm. (Adapted from Wong & Shi, 2015).

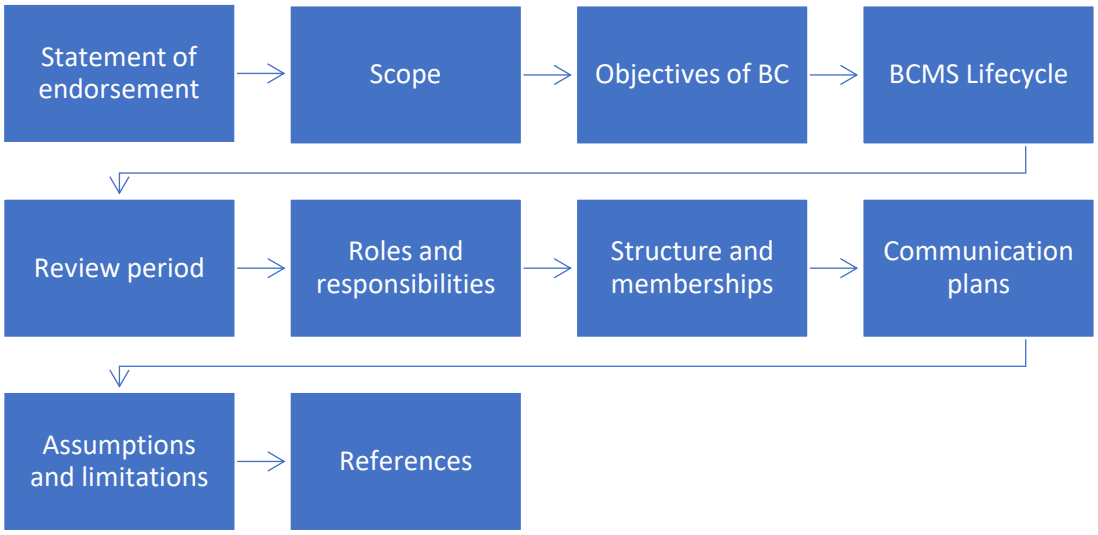
Clause 4 of the PDCA cycle sets out the requirements for specifying the context of the BCMS for the organization, including any needs, conditions, and scope. Clause 5 outlines the requirements for top management's role in the BCMS and how leadership communicates expectations to the organization through a policy statement. Finally, Clause 6 outlines the requirements for creating strategic objectives and guiding principles to shape the BCMS (ISO, 2019).

Business Continuity Policy

A business continuity policy is an official record that outlines the main components of an organization's Business Continuity Management System (BCMS). Specifically, the policy will typically include the following: a statement of endorsement; scope of the BCMS; objectives of business continuity; BCMS lifecycle; review period; delineation of roles and responsibilities; structure and membership; communication plans; accepted assumptions and limitations; and references (Wong & Shi, 2015).

Figure 7

Business Continuity Policy



Note. Figure 7 highlights the critical components of a business continuity policy.

A formal statement of endorsement by an executive leader, such as the chief executive, should reflect executive management's commitment to the Business Continuity Management System (BCMS). This statement should include the corporate definition of business continuity and outline how the organization applies the management process.

A business continuity policy must be tailored to the organization's specific needs, setting goals for successfully implementing the Business Continuity Management System (BCMS). The policy must ensure that all relevant legal and regulatory requirements are met and a commitment to ongoing review and improvement of the BCMS (ISO, 2019, p.8).

The scope of a BCMS is an essential factor in the overall implementation of the system. The content is determined either by a BCMS scoping analysis or a decision by the executives. It involves three key components: breadth, depth, and corporate resources. Breadth is the extent of coverage of the BCMS, depth is the degree of necessary planning activities, and corporate resources refer to the organizational assets required to make the BCMS a reality. The significance of developing and implementing a comprehensive business continuity plan was illustrated in a study by Margherita & Heikkilä (2021). The study leveraged a content analysis methodology to analyze web-based data on how the selected 50 corporations from 2019's Fortune Global 500 ranking responded to COVI9-19.

Content analysis is a popular methodology in social sciences because of its non-invasive nature. The method has been successfully used to investigate various topics. For instance, Maatota et al. (2019) conducted a content analysis of brand archetypes and storytelling components in LinkedIn ads (Margherita

& Heikkilä, 2021). A similar study by Parsons (2013), as cited by Margherita & Heikkilä (2021), performed a content analysis of Facebook pages to explore how companies would maximize social media to reach more customers.

A business continuity policy is an organizational strategy that outlines how an organization will respond and recover from potential threats such as natural disasters, pandemics, and cyber-attacks. A business continuity policy can help an organization anticipate, plan, and prepare for potential hazards. A business continuity policy must be documented and made accessible to all relevant personnel and interested external parties, as applicable (ISO, 2019, p.9).

Moreover, communicating a business continuity policy to employees helps create a culture of preparedness, allowing employees to understand their roles in a crisis and helping to ensure the organization is better equipped to respond quickly and effectively (ISO, 2019). In addition, it can help reduce the costs associated with downtime and the risk of reputational damage. Communicating a business continuity policy can help an organization protect itself from potential threats and ensure that it is prepared for any situation.

Lastly, the reference section should provide a comprehensive overview of the BCM standards the organization aims to achieve. Likewise, it should succinctly describe these standards and the rationale behind their adoption (Wong & Shi, 2015; ISO, 2019). The section should emphasize the connection between the BCMS and corporate governance and indicate where additional resources can be accessed.

Case Study of Hazards and Disasters Affecting BCP in IT-Driven Companies

Technological Disruptions

The repercussions for businesses can be substantial, from disruption of operations to data loss and even the potential collapse of the enterprise. In the past two decades, our perceptions of technological disruptions have evolved. Cyberattacks have become increasingly frequent and varied, ranging from denial-of-service attacks to ransomware and large-scale phishing operations to obtain confidential information. In 2018, cybercriminals targeted hospitals around the globe, causing both financial losses and disruptions to services. Hospitals in the United States, Ohio, and West Virginia were forced to divert ambulances from their emergency rooms due to ransomware attacks (Mathews, 2018, as cited in Phillips & Landahl, 2020). Although the damage was temporary, this event raised awareness of the potential threats of cyber-attacks to business continuity operations.

Space weather has become a significant concern in recent years due to its ability to disrupt technological systems. Geomagnetic storms and similar events can interfere with GPS and navigational techniques used by the airline and maritime industries, disrupt cellular services, and cause instability within power grids. As a result, the effects of space weather on businesses and their operations cannot be understated. In 2017, a major solar flare was recorded, resulting in a decreased positioning accuracy for satellites (Berdermann et al., 2018). The reverberations of this event could also be felt in the aviation and maritime industries, which rely heavily on navigational capabilities. This phenomenon is not new, as it was first observed in 1859 when a geomagnetic storm during the Carrington Event disrupted telegraph services, leading to one fatality and several injuries (Henderson et al., 2017).

A geomagnetic storm today could lead to a cascading event, wherein the consequences of one event trigger a sequence of more possibilities. Such an event might disrupt naval and military forces' communications networks or even affect the power grids responsible for the operation of other related services (Pescaroli et al., 2017). There is a fear that the aging electrical grid infrastructure along the East Coast of the United

States could be wiped out by a storm such as Carrington. The ramifications of this occurring during the winter could be dire for individuals and businesses. Therefore, the possibility of such disasters indicates that IT-driven companies must invest more in highly resilient business continuity and disaster recovery strategies.

Terrorism and Active Attacks

The recent terrorist attacks in Las Vegas and New Zealand demonstrate that no place or entity is immune to the disruption and destruction caused by terrorism, whether domestic or international. From workplaces to universities, ports to recreational facilities, and even places of worship, no business, agency, or organization can afford to ignore the risk of violence perpetrated by disgruntled employees or family members (Phillips & Landahl, 2020, p.11).

Notwithstanding, organizations must be prepared for the inevitable disruptions caused by mass shootings, acts of violence, cyber-attacks, ransomware, etc. Business continuity planning should be centered on quickly and effectively restoring regular operations following an event. According to Phillips & Landahl (2020), it is essential to consider the physical damage and the psychological trauma that may be inflicted to ensure a triumphant return to normal operations. Organizations can benefit from activating their employee assistance programs, which provide access to counseling and support from human resources regarding health care benefits and leave options to help employees manage physical, psychological, and spiritual distress.

In the wake of the 2017 terror attack on London Bridge, Borough Market was re-opened with a moment of silence. Prayer services were held to mark the re-opening of the businesses (Phillips & Landahl, 2020). The 2008 attack on a hotel in Mumbai, India, took three weeks to resume operations and nearly a year to repair the most heavily damaged sections. Business continuity planning is essential for addressing the human impacts of terrorism and the difficulty associated with re-opening after such a devastating event. Computer scientists and machine learners must understand the importance of such planning to help companies prepare for unforeseen circumstances.

P

andemics

The 1918 influenza pandemic is a stark reminder of the potential devastation that pandemics can cause. Fifty million people were killed in three waves over two years (Niall, Johnson, & Mueller, 2002, as cited in Phillips & Landahl, 2020). It is now easier to understand why people were encouraged to stay away from work to limit the spread of the Coronavirus. With the waning effectiveness of antibiotics and the potential for global transmission of infectious diseases, businesses need to be prepared for interruptions due to pandemics.

The 2014 Ebola outbreak in the US and Europe revealed how even a limited number of cases could have an extensive impact. The fear of the highly contagious virus spreading through air travel triggered a decrease in public confidence. Several airlines suspended flights to and from the affected countries (Amankwah-Amoah, 2016, as cited in Phillips & Landahl, 2020). The disasters demonstrate how small-scale events can have a significant disruptive effect, highlighting the importance of preventing the spread of disease.

SARS spread to 30 countries within half a year, significantly impacting certain regions, such as Hong Kong, Singapore, Vietnam, and Canada. Simple strategies like early detection and proper hygiene could have made a big difference, thus emphasizing the importance of preventive measures like flu shots and

handwashing for businesses in customer-facing roles, particularly educational establishments (Phillips & Landahl, 2020). In 2020, the global community was faced with the stark reality that an outbreak of an infectious disease can lead to quarantine in any given workplace or educational setting. The COVID-19 pandemic made this abundantly clear, with the virus claiming the lives of hundreds of thousands of people. Business continuity planning is essential to ensure that a business can withstand potentially catastrophic economic consequences, such as those posed by the COVID-19 pandemic. Such plans should include measures to safeguard the health of the workforce and the wider community.

Hurricanes and Cyclones

In 2017, Hurricane Maria severely impacted Puerto Rico, leading to substantial losses for businesses of all sizes. A survey by the Federal Reserve Bank of New York in 2018 revealed that 77% of companies experienced significant losses. These businesses faced a combination of reduced revenues, increased expenses, damaged assets, property damage, and an accumulation of debt (Hamdani et al., 2018). The survey revealed that over one-third of these businesses had no insurance coverage, while only 6% of those with insurance had their claims fully met (Hamdani et al., 2018).

In the wake of Cyclone Winston, which occurred one year prior, Fiji experienced catastrophic devastation in the form of damage to its people, homes, businesses, schools, infrastructure, and hospitals. This natural disaster, considered the worst storm ever recorded in the region, resulted in a significant economic impact: a loss of utilities, challenging roadways, and a struggling airport. Surprisingly, to make matters worse, 15% of the population was homeless, disrupting the labor force and causing an estimated $470 million in damages, or 10% of the nation's GDP (Aquino et al., 2018; Varandani, 2016).

Earthquakes

Earthquakes are a global phenomenon; unfortunately, not all countries or individuals are equipped to deal with the aftermath. The 2015 Nepal earthquake (measuring 7.8 on the Richter scale) resulted in a tragic death toll of close to 9000 people, with an additional 3.5 million people left homeless and economic losses of over 10 billion US dollars, significantly damaging the nation's gross domestic product (Goda et al., 2015). Nepal is also home to several World Heritage Sites, representing a source of income and employment opportunities for those supporting the tourism industry.

Nepal serves as a cautionary tale to illustrate the region's fragility and the potential need for economic assistance from governmental and non-governmental sources to sustain businesses' financial stability. UNESCO has taken a crucial step in the recovery process for the Kathmandu Valley by implementing an initiative to restore the region's tourism industry. This provides a potential source of income for individuals and enables them to revive their livelihoods, enabling them to rebuild and care for their families (Phillips & Landahl, 2020).

Volcanoes

In 2018, a volcanic eruption in Hawaii caused considerable economic impacts on tourism industries and significant losses to employers and workers regarding housing and businesses. This event serves as a reminder that, although volcanic eruptions may be less frequent than other types of natural hazards, the disruptions they cause can still be significant even at a distance.

The Eyjafjallajökull volcanic eruption of 2010 exemplifies natural hazards' profound and far-reaching impacts on businesses. Not only did the airlines experience direct implications in the form of airspace

closures and repairs, but the disruption to regular operations had a ripple effect across the globe, affecting 10 million travelers, including business employees and tourists (Phillips & Landahl, 2020). The incident serves as a reminder of the importance of considering natural hazards when assessing the risks associated with conducting business operations.

Mount Zao in Japan is a region that has experienced volcanic activity, which could potentially damage the industries in the area. A survey revealed that business owners were unaware of the potential risks and did not trust the pre-eruption warning messages (Donovan et al., 2018). Predicting volcanic eruptions and earthquakes is incredibly challenging. The same can be said of tornadoes, as they often have a brief warning period and can either cause a direct hit or completely miss the building next to one destroyed. This unpredictability can make it difficult to know whether to plan for business disruptions. However, planning is advisable, as disasters can happen anytime, and businesses will be relieved that they have a plan in place.

BCM, Risk Management, Crisis Management, and Disaster Recovery

Business Continuity Management in an IT-driven Space

Business Continuity Management (BCM) is critical to successful projects, including IT-driven construction projects. BCM helps to reduce the risk of unforeseen events that can disrupt the project timeline, such as accidents, natural disasters, or supply chain disruptions. BCM helps project managers identify potential sources of risk and develop plans to mitigate those risks. BCM should be integrated into the project management process; this includes establishing risk management processes, developing contingency plans, monitoring progress, and conducting post-implementation reviews (Supriadi & Pheng, 2018). BCM should be regularly reviewed and updated to ensure it is up-to-date and effective. By doing so, organizations can reduce the risk of project disruption and ensure a successful outcome.

Business Continuity Management (BCM) is a comprehensive process to ensure an organization is prepared to handle any potential disruption to its operations. BCM is a proactive approach to mitigating the effects of disturbance and involves identifying, analyzing, and mitigating risks. It also includes developing a plan to ensure the organization can continue during a disruption. The pandemic compelled companies and learning institutions to deploy business continuity plans and systems to ensure the continuity of operations. According to Rasiah, Kaur, & Guptan (2020), higher learning institutions were at the forefront of deploying technology solutions to guarantee the continuity of learning. In Indonesia, for example, the government partnered with private agencies to deliver free online education. Applications such as SPADA for higher learning institutions facilitated the continuity of education despite the disruptions caused by the pandemic.

The study by Rasiah, Kaur, & Guptan (2020) shows that most students had a positive experience with online learning during the pandemic. The results are generalizable because they involved students from 74 universities. The positive experience with online learning shows the critical role played by technology in ensuring the continuity of education during the pandemic. Despite the benefits of deploying technology to support recovery and continuity of learning, institutions face numerous challenges. For instance, Rasiah, Kaur, & Guptan (2020) noted that e-learning lacks interactive engagement typical in a conventional learning environment. As a result, such challenges must be considered when deploying new technologies to achieve continuity in IT-driven environments during disruptions.

On the contrary, crisis management is a response to disruption and involves using strategies and techniques to mitigate the potential impact of the interruption. Communication with stakeholders, developing

strategies to minimize the effect of the disturbance, and implementing those strategies are vital (Supriadi & Pheng, 2018). Crisis management is a reactive approach focused on mitigating a disruption's effects after it has occurred.

Disaster recovery is restoring an organization's systems, data, and personnel after a disruption. It involves implementing strategies and techniques to ensure the organization's operations can resume quickly and effectively. Disaster recovery focuses on restoring the organization's operations to a pre-disruption state and is a reactive approach to dealing with disruption. Nawari & Ravindran (2019) emphasizes that disaster is an action that may threaten life, technology, environment, well-being, and properties. Advancements in technology continue to provide more innovative and effective disaster recovery and management strategies.

However, disasters such as Hurricanes Harvey and Irma that hit various states, including Texas and Florida, indicate the need for businesses to invest more in business continuity and disaster recovery systems and technologies (Nawari & Ravindran, 2019, p.2). Consequently, blockchain solutions are necessary to develop effective disaster recovery and management strategies and solutions.

Table 1

BCM, Risk Management, Crisis Management, and Disaster Recovery

	BCM	Risk Management	Crisis Management	Disaster Recovery
Primary Focus	BCM focuses on events that can potentially cause a significant business disruption.	Organizations need to identify and assess risks that may be present thoroughly and consider the likelihood and impact of each risk before responding.	It focuses on the immediate steps to take when an emergency arises- primarily concerned with the initial few hours of the incident, including key decision-makers.	An area of emphasis centers on utilizing technology to address issues caused by external circumstances.
Key Method	Business Impact Analysis	Risk Analysis and Assessment	Risk Analysis and Contingency Plan	Contingency Planning

Note. Table 1 presents the critical focus areas and methods used in BCP, risk management, crisis management, and disaster recovery (Adapted from Supriadi & Pheng, 2018, p.70).

Business Impact Analysis (BIA) is an essential process of assessing the potential effects of disruption on a business's operations. BIA involves identifying Critical Business Functions (CBFs) - those functions that are essential to the operation of the company - and Minimum Business Continuity Objectives (MBCOs) - the level of service needed to ensure the continuity of the CBFs (Supriadi & Pheng, 2018). Together, these processes provide the necessary information for organizations to develop plans to ensure business continuity and protect their operations from unexpected interruptions.

Risk analysis and assessment involve recognizing potential risks and evaluating the level of their possible occurrence, while risk response consists in deciding on the appropriate measures to mitigate or eliminate

these risks. Risk analysis and contingency planning involve identifying potential risks and developing strategies to manage those risks (Supriadi & Pheng, 2018). A vital component of this process is the ability to detect early warning signals that could indicate that a crisis is looming. Organizations can reduce the likelihood and severity of any potential problem by recognizing and responding to these signals promptly and effectively.

The sentiments by Supriadi & Pheng (2018) are consistent with the conclusions of Koonin (2020), showing that the key domains (Cs) for business pandemic planning are continuity, crew, customers, and community. However, a crucial gap identified is that though most IT-driven companies have business continuity plans, few have pandemic plans (Koonin, 2020, p.4). Most companies have not recently tested their programs' and strategies' feasibility and operationality.

Disaster Recovery in a Digitally Powered Environment

In today's digital era, businesses need to ensure the continuity of operations to remain competitive. Even the slightest disruption in service availability can result in substantial financial losses for companies like Amazon and Flipkart, as customers cannot complete transactions (CC). Besides, it can lead to a poor user experience, damaging an organization's reputation and brand image (Osama, 2019). In many cases, application downtime stemming from programming or functional problems can be addressed swiftly and only impact a portion of the application. On the other hand, if the interruption is caused by an infrastructure or system failure, the entire application is affected, and the developers cannot control it through practical means.

High availability (HA) and disaster recovery (DR) are essential to any business infrastructure. The type of HA and DR solution a company chooses is primarily determined by the service level agreement (SLA) in place (Osama, 2019). The SLA outlines the recovery point objective (RPO) and recovery time objective (RTO), vital metrics for disaster resilience. High availability is a concept that is essential in risk management. A study by Kure & Islam (2019) shows how critical infrastructure is vital in risk management planning in an IT-driven environment. For instance, critical infrastructure such as software and networks must be secured from cyber-attacks and threats to enhance availability.

High availability guarantees a predetermined operational performance level for a system or application by limiting the amount of downtime due to infrastructure or hardware failure. In the event of hardware failure, the application must be quickly transferred to an alternate system to ensure the hardware issue does not lead to application downtime. Such possibilities are essential when developing business continuity and risk management plans in an IT-driven company (Kure & Islam, 2019).

Moreover, to ensure high availability, it is crucial to replicate the production environment as closely as possible, including the same hardware components, memory, CPU, and other configurations. For optimal performance, the primary and standby databases should be located at an appropriate distance (Kumar et al., 2019, p.7). Having them too close together would not be beneficial while having them too far apart would result in increased latency when transferring data to the replicated site. Besides, the network connection to the primary/production environment must be flawless.

A database comprises memory and background processes, denoted as "instances." The physical files of the database can be accessed via the instance. From a database point of view, the physical data files and the database instance should be available to the functioning database (Kumar et al., 2019, p.8). When connecting to the database, a new session is established to the instance in the database and should remain

active until the user disconnects it. Thus, to ensure the continuous activity of the session, it should not be disconnected at any point.

Table 2
High Availability and Disaster Recovery

Required	Function
System upgrades	System upgrades, such as software, hardware, network, or storage, are essential for keeping a system up-to-date and running properly. However, these upgrades may require the system to be restarted, leading to application outages due to configuration changes.
Human errors	It is inescapable that humans are prone to error; however, it is possible to put safeguards in place to help mitigate the consequences of such mistakes. For instance, errors in deploying an application or code can lead to a complete system failure.
Security breaches	Cyber-attacks are becoming increasingly frequent, leading to prolonged inactivity as organizations work to identify and address a security breach.

Note. Table 2 presents sample scenarios where high availability and disaster recovery are vital (Adapted from Osama, 2019).

In the case of system upgrades, fortunately, if a High Availability (HA) setup is in place, it is possible to perform these upgrades with no downtime. To illustrate the need for high availability and disaster recovery in human errors, one could cite the GitLab outage of January 31st, 2017, caused by the accidental deletion of customer data from the primary database server, resulting in an 18-hour disruption of service (Osama, 2019). To minimize the disruption caused by cyber-attacks, moving the application to a secondary database server may be a successful strategy for a quicker return to normal operations.

Availability is a critical factor in high availability and disaster recovery. Availability or uptime measures how often a system or application is available within a given year. It is expressed in terms of the "Number of Nines" or the percentage of availability (Osama, 2019).

For example, a system with 90% availability (one nine) could tolerate a maximum of 36.5 hours of downtime in a year, while one with 99.999% availability (five nines) could only accept a maximum of 5.26 minutes of interruption annually.

Figure 8

Availability %	Downtime per year	Downtime per month	Downtime per week	Downtime per day
90% (“one nine”)	36.5 days	72 hours	16.8 hours	2.4 hours
95% (“one and a half nines”)	18.25 days	36 hours	8.4 hours	1.2 hours
97%	10.96 days	21.6 hours	5.04 hours	43.2 minutes
98%	7.30 days	14.4 hours	3.36 hours	28.8 minutes

99% ("two nines")	3.65 days	7.20 hours	1.68 hours	14.4 minutes
99.5% ("two and a half nines")	1.83 days	3.60 hours	50.4 minutes	7.2 minutes
99.8%	17.52 hours	86.23 minutes	20.16 minutes	2.88 minutes
99.9% ("three nines")	8.76 hours	43.8 minutes	10.1 minutes	1.44 minutes

Availability

Note. Figure 8 presents the availability percentage and downtime per year, month, week, and day (Adopted from Osama, 2019).

Recovery Time Objective (RTO)

Recovery Time Objective (RTO) measures the maximum time a business can tolerate an application being unavailable without incurring significant financial, reputation, or data loss. For example, in an RTO of one hour, the application should be back up and running within an hour. Any downtime that exceeds this one-hour threshold could have potentially catastrophic consequences.

The choice of a high availability (HA) and disaster recovery (DR) solution is dependent on the Recovery Time Objective (RTO) of the application. If the application has a four-hour RTO, it may be possible to recover the database using backups, provided they are taken regularly at intervals of two hours or less (Osama, 2019). However, if the RTO is reduced to 15 minutes, then backups alone will not suffice, and HA and DR solutions must be implemented.

When implementing high availability, organizations must consider cost-effectiveness, manageability, and a high return on investment. It is essential to construct a comprehensive system that considers unanticipated outages and planned downtime, all while meeting set service level expectations (Kumar et al., 2019, p.556). Organizations must define Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) and design the appropriate high-availability architecture.

Recovery Point Objective (RPO)

Recovery Point Objective (RPO) measures how much data loss an organization can tolerate during a disruption or outage. For instance, an RPO of one hour would mean that any data loss within that time is acceptable, whereas any loss beyond that threshold could have significant financial or reputational consequences. The selection of a high availability (HA) and disaster recovery (DR) solution is contingent upon the Recovery Point Objective (RPO). Full daily backups are sufficient if an application requires a 24-hour RPO; however, if the RPO is significantly shorter, such as three hours, then full daily backups are inadequate (Osama, 2019).

The following scenario illustrates the difference between RPO and RTO. A company has an RTO of 2 hours and an RPO of four hours, with no High Availability (HA) or Disaster Recovery (DR) solution. The backups are carried out every 6 hours. If the system experiences an outage, the database could be restored from the last full backup within the RTO of 2 hours. However, the data loss would be more than four hours due to the 6-hour backup interval exceeding the given four-hour RPO.

Case Studies: Oracle Public Cloud and Microsoft Azure

Disaster Recovery with Oracle Public Cloud

The Oracle Cloud Infrastructure offers a convenient deployment model with several selections for datab-

ase implementation, such as Active Data Guard and Real Application Clusters with a platform as a service license. The user can bring their license to the Oracle Cloud Infrastructure. The Oracle public cloud offers an invaluable cloud-bursting capability and on-demand elasticity solution while providing a secure environment where data is consistently validated to prevent inconsistency or corruption (Kumar et al., 2019, p.557). As a result, users may be interested in leveraging the Oracle public cloud as a disaster recovery solution for their on-premises databases or creating a DR solution for a database already hosted on the cloud.

Disaster Recovery with Microsoft Azure

By leveraging the features and services Microsoft Azure provides, users can make critical applications more resilient by planning and designing a secondary recovery system in Azure. This implementation will enable applications to achieve greater availability in the cloud via Azure-based tools and services.

In conjunction with platform resiliency, Microsoft Azure services redefine the cloud data recovery concept. Instead of being limited to recovery-only, Microsoft sets a new standard with availability on demand, enabling users to recover data whenever needed, with the assurance that the necessary data is always available.

Once a connection from the data center to Azure is set up, servers can be replicated using Azure, like a custom recovery or backup solution. Placing data in Azure can benefit from the security of having Azure as an alternate site in an emergency and take full advantage of Azure's strong computing and storage possibilities (Chakraborty & Chowdhury, 2020). With the data already in Azure, setting up a replicated workload in Azure for DevTest, or assigning a larger Azure template to offer extra computing power is just a few clicks away, with no impact on the in-house production workload.

Resiliency is paramount regardless of where systems are located, whether on-premises or in the cloud. Systems, especially in an IT-driven environment, must withstand both minor and major failures, with the capacity to handle transient failures and losses at multiple levels, such as hardware, service, or specific tier failure. When entire data centers or even whole regions experience an uncontrollable event, a reliable recovery solution should be in place to restore systems and ensure continued business operations swiftly.

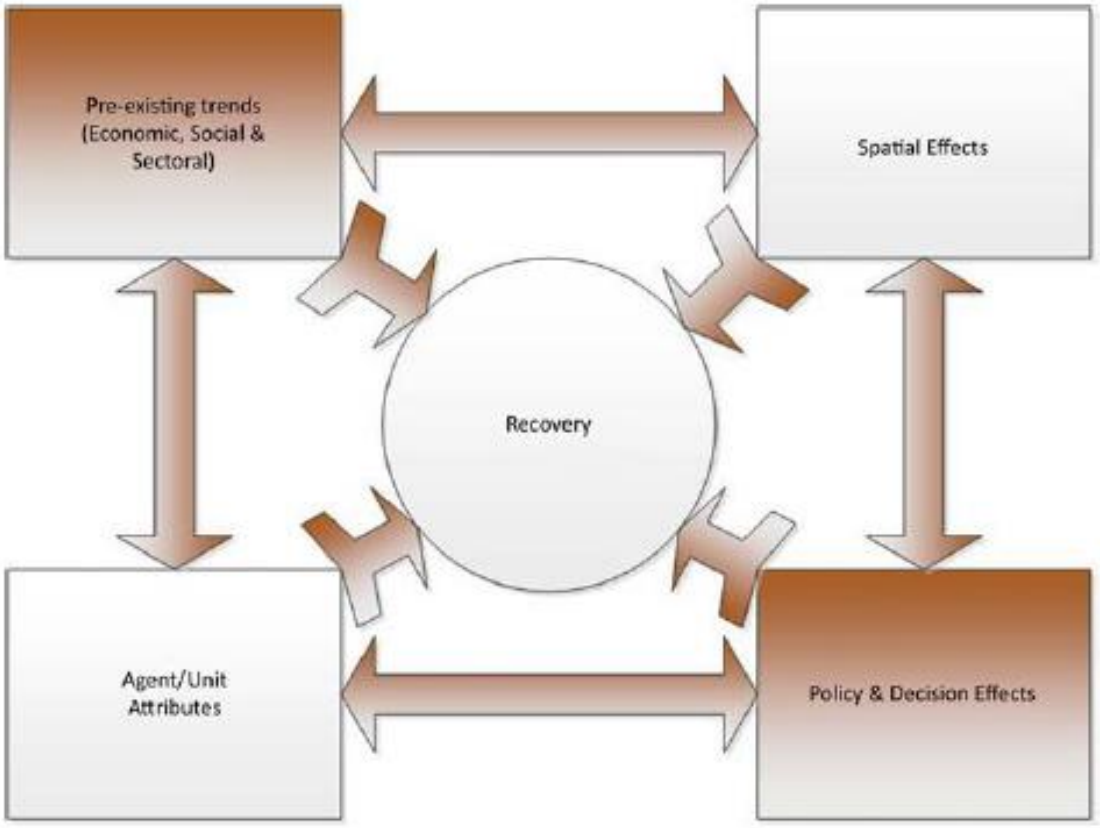
Microsoft Azure provides two critical services in addition to the essential components already discussed: Azure Backup and Azure Site Recovery (ASR). Azure Backup is a cloud-based backup solution that protects on-premises and cloud-deployed resources. On the other hand, ASR facilitates replicating virtual machines between on-premises and Azure to create an identical copy of resources that can be made available online for disaster recovery (Chakraborty & Chowdhury, 2020, p.40). Besides, it can be integrated with SQL Always On Availability groups for failover and failback by creating DR plans.

Business Recovery from Disaster: Creating an Enabling IT-Environment

Businesses do not just survive or fail because of disasters; corporate decisions determine their success before and after a disaster. These decisions are significantly impacted by pre-existing institutional, social, and sectoral trends and policy interventions enacted to facilitate recovery post-disaster (Hatton, Vargo, & Seville, 2023).

Figure 9

Interrelated Recovery Influences



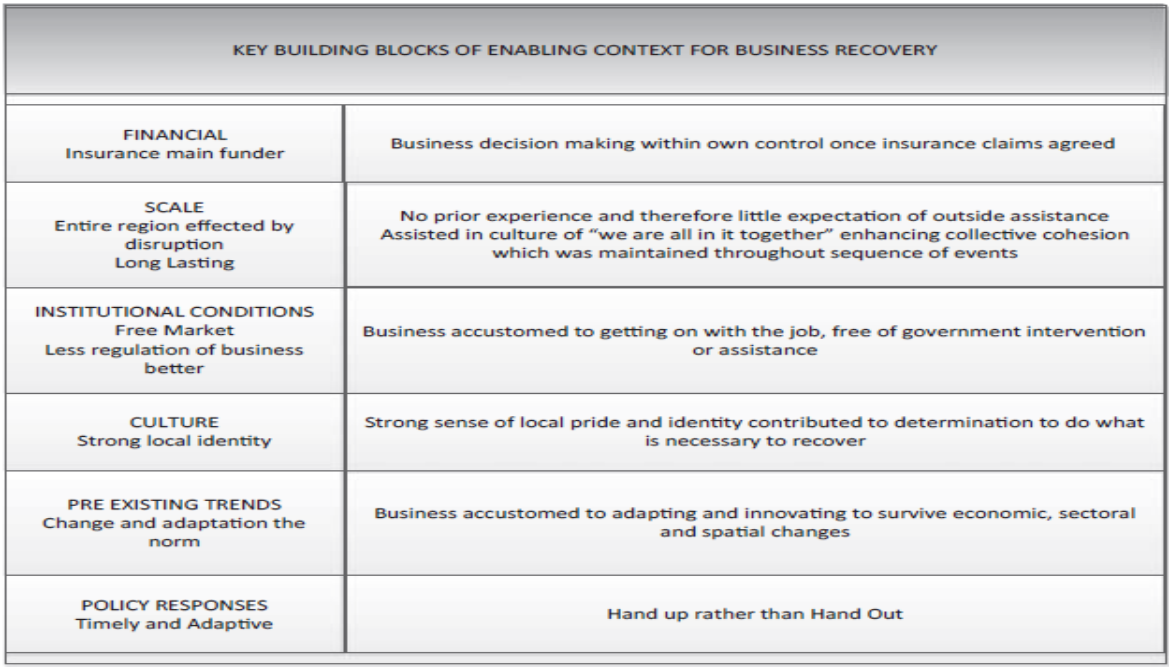
(Hatton, Vargo, & Seville, 2023, p.5)

Figure 9 illustrates the five major interrelated recovery influences. These influences encompass pre-existing economic and social trends, the attributes of agents or units, the impact of spatial effects, and the power of policy or decision-making (Miles and Chang, 2006, as cited in Hatton, Vargo, & Seville, 2023). The fifth influence mentioned is the multiple interactions between these areas, as illustrated by the multi-directional arrows.

A thorough comprehension of the impacts of business decisions in disaster environments can enable those responsible for disaster response to anticipate the potential outcomes and identify the most suitable interventions to help communities recover from extreme events. Hatton, Vargo, & Seville (2023) assert that most research focuses on organizational traits that may potentially influence business recovery after a disaster has been conducted, but contextual factors' effects are insufficiently explored.

An enabling environment that encourages individuals, organizations, and communities to lead their recovery efforts while providing the necessary support and coordination functions is a highly intricate undertaking (Hatton, Vargo, & Seville, 2023).

Figure 10



KEY BUILDING BLOCKS OF ENABLING CONTEXT FOR BUSINESS RECOVERY	
FINANCIAL Insurance main funder	Business decision making within own control once insurance claims agreed
SCALE Entire region effected by disruption Long Lasting	No prior experience and therefore little expectation of outside assistance Assisted in culture of "we are all in it together" enhancing collective cohesion which was maintained throughout sequence of events
INSTITUTIONAL CONDITIONS Free Market Less regulation of business better	Business accustomed to getting on with the job, free of government intervention or assistance
CULTURE Strong local identity	Strong sense of local pride and identity contributed to determination to do what is necessary to recover
PRE EXISTING TRENDS Change and adaptation the norm	Business accustomed to adapting and innovating to survive economic, sectoral and spatial changes
POLICY RESPONSES Timely and Adaptive	Hand up rather than Hand Out

Building Blocks for Business Recovery

Note. Figure 10 illustrates the crucial components that enabled Canterbury to foster individual, organization, and community-driven recovery initiatives (Adopted from Hatton, Vargo, & Seville, 2023).

The independence of business fostered by years of free market focus, paired with the availability of high levels of insurance, led to an enabling context for recovery (Hatton, Vargo, & Seville, 2023). By providing businesses with the means to fund their recovery efforts, these insurance payments allowed them to take control of their destiny and create a sense of certainty in the wake of the event.

Disaster recovery practitioners should create horizontal and vertical integration to foster inter-organizational collaboration. Horizontal integration focuses on connections between local government representatives, small businesses, media outlets, community groups, and residents (Smith, 2011, as cited in Hatton, Vargo, & Seville, 2023). When a community has inadequate horizontal integration, achieving a unified vision of recovery can be difficult. Vertical integration involves connections between local and state governments, private entities, and non-governmental organizations, improving their capacity to respond to disasters.

Berke, Kartez, & Wenger (1993), cited in Hatton, Vargo, & Seville (2023), suggested that communities with a high degree of horizontal and vertical integration are likely to experience a quicker rate of recovery from disasters. The research suggested practical recommendations for increasing integration throughout the disaster recovery network. Such integration would prevent duplication of efforts, reduce the chances of conflicting actions, and optimize the use of resources, thereby allowing a much swifter and more extensive recovery.

A study by Schmidt, Garland, & Quebedeaux (2023) explored a sample of faith-based and secular nonprofit organizations in the 11-county Upper Texas Gulf Coast region. This region encompasses Harris and surrounding counties stretching from Brazoria to Orange and Galveston to San Jacinto. The initial dataset included 26,000 organizations sourced from Infogroup and Urban Institute data.

In Schmidt, Garland, & Quebedeaux's (2023) study, a stratified sample of 3,538 faith-based and secular nonprofit organizations (FBSNOs) was selected to receive phone surveys, while an additional 450 organizations received a link to an online survey. In addition, 38 in-depth, face-to-face interviews were conducted with FBSNOs, foundations, and federal, state, and local government officials. The survey questionnaire aimed to identify the characteristics of FBSNOs participating in disaster response and recovery and the services they provided in response to Hurricane Ike.

The response rate to all forms of surveys was meager. A few organizations declined to participate, citing that they did not want to be involved, were hesitant to release confidential information, or did not have the resources or time to complete the online survey. Notably, most contacted organizations were small, no-budget organizations and had answered many surveys.

Organizations that responded to the survey reported providing a range of services. These services were supplied directly or through collaboration with other agencies. The survey revealed that the most provided services were related to monetary/in-kind donations, clothing/home goods/furnishings, and food centers. However, the few surveyed organizations offered long-term housing, childcare, and job training (Quebedeaux, 2013, as cited by Schmidt, Garland, & Quebedeaux, 2023).

Figure 11

Recovery Services Provided

	Directly	In support of another agency or organization
Health care	10	12
Mental care or counseling	9	11
Child care	6	4
Job training	1	5
Food centers/ice	20	14
Temporary housing	11	13
Long-term housing	3	7
Clothing/housewares/furniture	26	11
Transportation/communication	15	8
Money/in kind donations	28	15
Counseling for applying for assistance	14	7

Note. Figure 11 shows the recovery services provided directly and in support of other agencies (Adopted from Schmidt, Garland, & Quebedeaux, 2023).

In-depth interviews validated the services listed by FBSNOs in the survey and further revealed the provision of additional services, such as medical and psychological aid, running of shelters, food, and ice centers, help with long-term housing and domestic supplies, transportation, communication, direct contributions, and case management (Quebedeaux, 2013). Several FBSNOs voiced difficulties concerning horizontal and vertical integration in the disaster recovery system (Schmidt, Garland, & Quebedeaux, 2023). Also, social services were absent during disaster response and recovery, as local and state governments focused on infrastructure and businesses. In contrast, people and housing often do not get the same attention in response and recovery strategies.

Furthermore, the interviews revealed a lack of uniformity and harmony between government agencies and issues accessing reliable disaster-related data. Besides, multiple governmental organizations conducted

similar reviews and gathered the same information but did not share the collected data (Quebedeaux, 2013, as cited in Schmidt, Garland, & Quebedeaux, 2023). As a result, a lack of data sharing could adversely hinder the development and execution of effective business continuity plans, especially in an IT-driven business environment.

Challenges to Implement Business Continuity Management

Various literature explains the challenges to BCP management. In "Framing business continuity to achieve lasting focus" by Zawada and Perry (2020), the authors argue that traditional BCP approaches, which often rely on reactive measures such as disaster recovery plans, are insufficient in today's rapidly changing business landscape. They highlight the role of leadership and culture in achieving effective BCP. They argue that organizations must create a culture of resilience where all employees understand the importance of BCP and are actively engaged in the process. Additionally, senior leaders must prioritize BCP and allocate the necessary resources to ensure its success – which is not occurring in today's average organization.

Business Continuity Plans (BCPs) must be incorporated into the core principles of any Fortune 500 company. The authors suggest a new framework for BCP that integrates risk management and organizational resilience into the planning process. This approach helps organizations prepare for and respond to disruptions and improves their competitiveness and ability to adapt to changing conditions. The authors emphasize the importance of considering internal and external factors when developing a BCP plan, including technology, supply chain management, and regulatory compliance. The authors' emphasis on integrating risk management, organizational resilience, and cultural considerations into the BCP process is a timely and essential contribution to the field. This article is a valuable resource for organizations looking to enhance their BCP efforts and achieve lasting focus in today's rapidly changing business landscape. However, despite all the standards-based guidelines and government directives, corporations and public companies pay little relevance to implement BCPs. Thus, during an unforeseen business interruption due to an uncontrollable event such as a natural disaster or pandemic, these companies, and the country's economy, will take a huge hit (Zawada & Perry, 2020).

The Complexity

Filipović et al. (2021) surveyed Croatian organizations to understand their current BCM practices and the impact of crisis events on their approach to BCM. The survey results indicate that while many organizations have developed BCM plans, their implementation and effectiveness are limited due to the complexity of effective BCPs. The authors found that due to the complex nature, organizations prioritize immediate recovery rather than long-term resilience, which can limit their ability to respond to future crises effectively. The authors also found that the COVID-19 pandemic has had a significant impact on the development of BCM in Croatia. Many organizations have quickly implemented remote work policies and procedures to ensure business continuity. The authors argue that the pandemic has highlighted the need for organizations to prioritize technology and digital infrastructure in their BCM planning. Development of BCM in Croatia has been slow but has been accelerated by crisis events such as the COVID-19 pandemic. They suggest that organizations must prioritize long-term resilience and invest in technology and digital infrastructure to ensure effective BCM in the future.

Lack of Tools and Resources

In their pre-pandemic book titled business continuity and disaster recovery planning for IT Professionals, the authors Campbell & Brown (2015) provide valuable insights into the impact of IT and digital technology on business continuity planning and the challenges and opportunities it presents. The authors argue that the increasing reliance on technology in organizations has made it more critical than ever to have effective BCP in place. However, they found that many organizations lack the tools and technology to support BCP. The authors suggest that organizations invest in technology and tools that support BCP to ensure they are prepared for disruptive events. The authors offer practical recommendations for organizations looking to incorporate digital technologies into their BCP strategies and effectively manage the new risks and opportunities that arise in the digital age.

Campbell & Brown (2015) thoroughly examines the impact of information technology on business continuity planning (BCP) in the modern era. The authors aim to identify the challenges and opportunities that digital technology presents for BCP and provide insights into how organizations can effectively incorporate digital technologies into their strategies. One of the study's key findings is that information technology has significantly changed the nature of business continuity planning, with new risks and opportunities arising. For example, the authors note that information technologies such as cloud computing and automation can significantly enhance the ability of organizations to respond to disruptions but also present new risks such as data breaches and cyber-attacks.

Lack of Awareness & Training

Campbell & Brown (2015) also finds that organizations must adopt a comprehensive and integrated approach to BCP to manage these new risks effectively. This includes incorporating digital technologies into their BCP strategies and ensuring their plans are regularly reviewed and updated to consider unknown risks and technological advancements. The authors also highlight the importance of involving all relevant stakeholders in the BCP process, including employees, customers, and suppliers. All stakeholders must be aware of their role during a disruption. It is crucial to ensure that the BCP plan is aligned with the needs and expectations of all parties.

Lessons learned from the COVID-19 pandemic.

Margherita & Heikkilä (2021) published a research paper that explores the measures taken by world-leading companies to maintain business continuity during the COVID-19 pandemic. The article provides a comprehensive overview of companies' actions in response to the pandemic, including remote work arrangements, supply chain management, and crisis management. The authors used a qualitative research design to collect data through interviews with senior executives from leading companies. The research findings showed that companies were proactive in responding to the pandemic and could effectively manage the crisis by adapting to the new circumstances. Unfortunately, most of our Fortune 500 companies didn't reach the safe list.

One of the critical findings of Margherita & Heikkilä (2021) is the importance of effective communication and collaboration in times of crisis. Companies that could effectively communicate and collaborate with their employees, customers, and suppliers could maintain business continuity, while those that struggled with communication and collaboration faced significant challenges. The study by Margherita & Heikkilä (2021) also found the importance of technology and digitalization in maintaining business continuity during the pandemic. Companies that had already embraced technology and digitalization were better

equipped to adapt to the new circumstances and maintain business continuity. In contrast, those that were slow to adopt technology struggled to keep pace.

The paper is well-written and provides a comprehensive overview of the actions taken by leading companies during the pandemic. The authors also discuss the role of government and regulatory bodies in ensuring business continuity during the pandemic. They highlight the importance of clear and consistent regulations and guidelines in effectively helping companies respond to the crisis. Their research findings can serve as a helpful guide for companies looking to improve their business continuity planning in response to future disasters.

Vogel (2022) also researched BCPs with a COVID-19 backdrop and provided valuable insights into the importance of validating business continuity programs in the face of the pandemic's new normal. The authors argue that the COVID-19 pandemic has highlighted the need for organizations to reassess and validate their business continuity programs to ensure they are practical and up to date in the new normal. The article provides a detailed analysis of the critical elements of a successful validation program, including risk assessment, scenario testing, and stakeholder engagement. The authors also offer practical tips and guidance on effectively implementing a validation program, including documenting the process and outcomes.

While both articles offer valuable insights into business continuity, their focus, and approach differ. The article "*Validating Business Continuity Programs in the New Normal" by* Vogel (2022) focuses on the importance of validating business continuity programs in the new normal, while the article *Business Continuity in the COVID-19 Emergency: A Framework of Actions Undertaken by World-Leading Companies* by Margherita & Heikkilä (2021) focuses on the actions taken by world-leading companies to manage business continuity during the COVID-19 pandemic.

Proposals from current literature

A few proposals, guidelines, and alternative solutions may be extracted from the currently available literature to solve this problem. The article, *Clinical Practices for Business Continuity Planning*, published on the Yale School of Public Health Emergency Management website, provides a comprehensive overview of best practices for clinical organizations to develop and implement a business continuity plan (BCP). The university aims to help clinical organizations prepare for emergencies and minimize the potential negative impacts on patient care and services. The article discusses the steps involved in developing and implementing a BCP, including risk assessment, business impact analysis, development of strategies, and testing and maintenance. The authors explain the risk assessment process, which involves identifying potential threats and assessing their likelihood and potential impact. The article also discusses the importance of business impact analysis, which evaluates the effect of possible disruption on the organization's operations and services.

On a very similar note, the Federal Emergency Management Agency (FEMA) has published a toolkit on its website - Continuity Resource Toolkit (2020), which appears to be a comprehensive online resource designed to assist organizations in developing and implementing practical business continuity plans (BCP). The toolkit provides a step-by-step guide to the BCP process, including risk assessment, business impact analysis, and developing strategies for managing emergencies.

Just like Yale University (2019), Continuity Resource Toolkit (2020) also provides an overview of the critical elements of a BCP, and the steps involved in the development process, including risk assessment, business impact analysis, and the development of strategies for managing emergencies. The risk

assessment section of the toolkit provides practical guidance on identifying potential threats and assessing their likelihood and potential impact. However, unlike Yale University (2019), Continuity Resource Toolkit (2020) provides a comprehensive strategy in the business impact analysis section and offers a step-by-step guide for evaluating the impact of a potential disruption on the organization's operations and services. The toolkit also provides a comprehensive guide to developing emergency management strategies, including contingency planning, backup and recovery planning, and crisis communication planning. The authors provide practical examples and templates to assist organizations in developing effective strategies.

Customer engagement for BCPs.

Kaur et al. (2021) highlight the impact of customer engagement on business continuity in the context of sustainable supply chain management. The authors explore the role of customer engagement in mitigating the risk of supply chain disruptions and enhancing the resilience of organizations in the face of such disturbances. One of the study's key findings is that customer engagement is a critical enabler of business continuity in supply chain management. The authors argue that organizations can benefit from the insights and feedback provided by their customers to identify potential risks, prioritize their response strategies, and enhance their resilience to supply chain disruptions. Furthermore, the authors note that customer engagement can help organizations to build trust, establish long-term relationships, and foster collaboration and cooperation, which are critical components of a sustainable and resilient supply chain.

Kaur et al. (2021) also provide practical recommendations for organizations to engage their customers in supply chain management effectively. These recommendations include creating a customer engagement strategy, integrating customer feedback into supply chain management processes, and fostering a culture of openness and transparency. The authors also emphasize the importance of using technology, such as digital platforms and social media, to enhance customer engagement and facilitate real-time communication and collaboration. The study is based on a comprehensive review of the existing literature and includes several case studies that illustrate the impact of customer engagement on business continuity in supply chain management. The authors provide a clear and well-structured argument, and the evidence supports the findings and recommendations presented in the article.

The Shift from Planning-driven to anticipated improvisation.

Groenendaal & Helsloot (2019) presents a thought-provoking analysis of the evolution of business continuity management and the need for organizations to shift towards a more resilient approach. The author argues that traditional planning-driven business continuity management approaches are no longer sufficient in the face of increasing uncertainty and complexity and that organizations must adopt a more adaptive and improvisational approach to resilience instead.

The authors define organizational resilience and its key components: agility, adaptability, and anticipatory capacity. They then go on to discuss the limitations of traditional business continuity management approaches and the reasons why they are no longer adequate. The authors also highlight the importance of developing anticipatory capacities and the role of improvisation in achieving organizational resilience (Groenendaal & Helsloot, 2019).

Groenendaal & Helsloot (2019) also thoroughly examine the benefits of adopting an improvisational approach to organizational resilience and the key elements that must be in place for it to be effective. The

author also provides case studies and practical examples to illustrate the benefits of this approach and how it can be applied in different organizational contexts.

A quantitative framework Vs. Adaptive agility for BCPs.

Soufi et al. (2019) propose a quantitative framework that provides a systematic and structured approach to assessing and managing risks associated with business disruptions. The framework is designed to help organizations make data-driven decisions about their business continuity plans, making them more effective and efficient. The authors begin by discussing the limitations of traditional business continuity planning approaches and the need for a more structured and quantitative approach. They then introduce the critical components of their framework, including risk assessment, risk management, and performance monitoring. The authors also explain how the framework can be used in practice, using case studies and examples to illustrate its effectiveness. The article is well-researched and provides a comprehensive analysis of the benefits of the proposed framework. The authors have done an excellent job presenting the framework clearly and concisely, making it easy for practitioners to understand and implement. The authors also highlight the importance of continuous monitoring and updating business continuity plans to ensure their relevance and effectiveness over time.

Hatton & Brown (2021) suggest a related solution in their article titled Building Adaptive Business Continuity Plans: Practical Tips on *Inject Adaptiveness into Continuity Planning Processes*, published in the Journal of Business Continuity and Emergency Planning. They provide valuable insights into incorporating adaptiveness into business continuity planning processes. The authors argue that traditional continuity planning approaches, which focus on planning and preparation, are no longer sufficient in rapidly changing and uncertain business environments. Instead, organizations must adopt a more adaptive and agile approach to business continuity planning. They provide practical tips and guidance on injecting adaptiveness into continuity planning processes, including the importance of stakeholder engagement, risk assessment, and continuous monitoring and review.

Soufi et al. (2019) and Hatton & Brown (2021) offer valuable insights into business continuity planning but differ in their focus and approach. Hatton & Brown (2021) emphasizes the importance of adaptiveness and agility in business continuity planning, while Soufi et al. (2019) focus on the benefits of a quantitative, data-driven approach to risk management. They emphasize that a quantitative framework provides a structured method for analyzing and measuring a disruptive event's potential impact and determining the resources required to respond. This information can then be used to develop a comprehensive business continuity plan tailored to the organization’s specific needs. The authors also provide case studies and examples to illustrate the practical application of their approach.

The literature review performed in this paper highlights the importance of utilizing information systems for cost-effective business continuity planning. The literature demonstrates that organizations can streamline their continuity planning processes by implementing information systems and ensuring critical business functions and data are protected during disruptions. Information systems also facilitate regular testing and updating of continuity plans, reducing the costs associated with manual processes and improving overall preparedness. The literature emphasizes the importance of involving all stakeholders, including IT and business personnel, in developing and implementing the BCP. The objective is to ensure that all critical systems and processes are considered and that BCP is aligned with the organization’s overall strategy and goals. The findings indicate that organizations that invest in information systems for business continuity planning experience increased resilience and are better able to respond to disruptive

events, ultimately leading to cost savings and improved business outcomes. The literature supports using information systems as a crucial tool for effective and cost-efficient business continuity planning.

Methodology

Introduction

This chapter presents a comprehensive description and explanation of the methodology employed in this study. The research philosophy used is interpretivism, a philosophical stance with a heritage in the intellectual traditions of phenomenology and symbolic interactionism. Interpretivism is highly relevant to this study because of the complexity and richness of the use of information systems to create, deploy, test, and maintain business continuity plans and techniques in a digitized business environment. An inductive approach was employed to enhance the flexibility and adaptability as the research progresses, in contrast with a deduction which instills a rigid framework for conducting research. The research strategy employed is exploratory, executed using case studies. The multiple case study strategy focuses on IT-driven organizations operating in three distinct sectors: manufacturing, supply, and banking. The IT-driven companies have operations in Europe, the United States, China, and virtually globally. The findings of the case studies are combined with the findings of a survey on business continuity by the European Commission's Joint Research Center. Combining the case studies and the survey results provides sufficient data and conclusions to answer the research questions and achieve this study's objectives. The limitations of the methodology and ethical research practices embraced in this study are detailed.

Research Philosophy

Research philosophy relates to the development and nature of knowledge. Any research study is an endeavor to develop proficiency in a specific field. Knowledge development is not necessarily dramatic as creating a new theory of motivation, but even a modest inspiration to solve a particular problem a given population faces. The ambition to answer specific research questions or test hypotheses amounts to developing new knowledge. The research philosophy employed by a researcher comprises essential assumptions about their worldview. The assumptions underpin the research strategy and methods for collecting and analyzing data to achieve the research objectives.

According to Saunders, Lewis, & Thornhill (2009), the philosophy adopted in research is influenced by practical factors and considerations. However, in most cases, research philosophy selection is controlled by the researcher's view on the link between knowledge and the process of developing it. A researcher concerned with factors, such as resources required to deploy a BCP system, will have a varied view from one concerned with the feelings and attitudes of employees towards implementing the BCP system to achieve operational efficiency and exceptional service delivery. The strategies and methods employed to collect and analyze data by these researchers will differ. Besides, the research process and their views on what is helpful to achieve their research objectives will vary.

The three primary categories of research philosophy are epistemology, ontology, and axiology. Each category comprises the unique assumptions and concepts shaping the research process. Epistemology concerns sufficient knowledge in a specific field of study (Saunders, Lewis, & Thornhill, 2009; Muhaise et al., 2020). The distinction can be better illustrated by the scenarios of two researchers with unique interests in implementing a new system to foster business continuity in an IT-driven organization such as a modern Healthcare facility. The researcher interested in the resources required for the successful implementation of the system will be more akin to the natural scientist position.

For instance, an operations management specialist will likely take such a position of interest in collecting and analyzing facts. For this researcher, the reality is represented by natural objects such as computers and network devices needed to deploy the business continuity management system successfully. According to the researcher, the data collected is more objective and less biased than the data collected by a researcher interested in the feelings and attitudes of employees regarding the deployment of the same system. The 'resources' researcher views the objects examined by the 'feelings' researcher as social phenomena with no external reality (Saunders, Lewis, & Thornhill, 2009). The ‘resources' researcher may only place authority on such data when presented statistically, in a table or graph. Presenting the data in tables lends more objectivity to the researcher's view.

Based on this insightful illustration, the 'resources' researcher embraces a positive position on knowledge development while the 'feelings' researcher adopts an interpretive perspective. The philosophical stance of interpretivism was adopted in this study to explore the information systems for business continuity planning in IT-powered organizations. Interpretivism is an epistemology advocating that the researcher understands the distinction between humans as social actors. Ganesha & Aithal (2022) provides a more comprehensive description of the connection between interpretivism and subjectivism. Researchers who adopt the interpretivism philosophical paradigm believe that the nature of reality (ontology) is rich and complex. They also believe that reality is a blend of unique experiences, practices, and processes (Ganesha & Aithal, 2022). As a result, this philosophical paradigm is relevant considering the complexity and richness of experiences regarding using information systems to accomplish business continuity in a digitized business space.

Researchers are critical of positivism, posit that rich insights into the complex world are lost if reduced to a series of law-like generalizations. The heritage of interpretivism is two intellectual traditions: phenomenology and symbolic interactionism (Saunders, Lewis, & Thornhill, 2009). Phenomenology concerns how humans make sense of the world, while symbolic interactionism is a continuous process of interpreting the social world. Interpretivism is a highly appropriate research philosophy in business and management research because business situations are complex and unique. According to Muhaise et al. (2020), interpretivism is unique because the researcher is involved in the research process. Besides, the researcher's interpretation contributes to the field of study. The philosophical stance of interpretivism is appropriate in this study because using information systems to create, test, execute, and maintain business continuity plans is complex and unique to different IT-driven organizations.

Research Approach

Researchers should not fall into the trap of thinking that one research approach is better than another. They must understand that research approaches are 'better' at doing unique things. The questions determine the 'better' research approach (Saunders, Lewis, & Thornhill, 2009). However, the practical reality is that no study neatly falls into one specific philosophical domain as recommended in the research 'onion' proposed by Saunders, Lewis, & Thornhill (2009). A research approach can be deductive or inductive. In a deductive research approach, the researcher develops theory and hypotheses and then designs a strategy to test the hypotheses. In an inductive approach, the researcher collects data to analyze and establish a theory. Muhaise et al. (2020) highlight how the researcher's worldview and philosophical stance shape the theories, approaches, methods, and instruments used in research. Therefore, the approach selected is guided by the principles of interpretivism, including the value of interpreting complex and rich reality.

An inductive approach was employed in this study. Understanding the role of information systems in creating, executing, testing, and maintaining business continuity plans requires getting a feel of what is happening in IT-driven companies using the technology. For instance, access to data from Fortune 500 companies will provide accurate insights into how information systems can be used to make the cost of BCPs affordable. The data will also provide insights into what can be done to educate large-scale organizations on the risks and costs of failing to implement adequate BCPs.

Followers of the inductive approach criticize deduction for the tendency to develop a rigid methodology blocking alternative explanations of what is going on regarding the research problem. Deduction creates an air of finality regarding the definition of the hypothesis and choice of theory (Saunders, Lewis, & Thornhill, 2009). Though alternative views may be developed, deduction restricts them within the limits of the highly structured design. However, some studies have integrated inductive and deductive approaches into thematic analysis and mixed-method research (Proudfoot, 2022). For instance, inductive methods have been successfully integrated with a thematic analysis strategy proposed by Braun and Clarke (Proudfoot, 2022). The complexity and uniqueness of using information systems to create, test, and execute BCP plans across different IT-powered organizations require an interpretive approach to enable a broader understanding and explanation of the current situation.

Table 3
Deductive vs. Inductive Approaches

Deduction Emphasizes	Induction Emphasizes
Scientific principles	Understanding of meanings attached to events by humans
Collection of quantitative data	Collection of qualitative data
Applications of controls to ensure data validity	Flexible structure to permit changes as research progresses
Researcher independence	Researcher as part of the research process
The sample selected sufficient to generalize conclusions	Less concern about generalization

Note. Table 3 provides the differences between inductive and deductive approaches to research.

Research Design

A research design is a general plan for answering the research questions. The design strategy depends on the researcher's preferences, philosophy, and the most appropriate data collection method. According to Yin (2018), a researcher should consider the form of the research questions, the control over behavioral events, and the contemporary nature of the events related to the study area before selecting a research design.

After considering the research questions, control over behavioral events, and other factors, this study is designed as exploratory research. An exploratory study is a practical design to discover what is happening, seek new insights, and ask questions to clarify a specific problem from a new perspective. This exploratory study focuses on exploring what is happening, developing new insights, and asking questions to clarify the role of information systems in creating, deploying, and executing BCPs in IT-driven organizations. Three principal ways of conducting exploratory research include literature searches, expert interviews, and case studies (Saunders, Lewis, & Thornhill, 2009; Smith & Albaum, 2012). The exploratory design

was selected because of its flexibility and adaptability to change and accommodate new data and insights. The inherent flexibility of exploratory analysis does not infer the absence of direction guiding the inquiry. Instead, it means the focus is initially broad but narrows as the research progresses.

Research Strategy

Selecting a clear research strategy is essential in any scientific inquiry. Various research strategies can be used to execute exploratory, descriptive, or explanatory research (Yin, 2003; as cited in Saunders, Lewis, & Thornhill, 2009). No research strategy is inherently inferior or superior to another. What is essential is to choose a research strategy that will answer the research questions and achieve the research objectives. The research questions, goals, extent of existing knowledge, and philosophical underpinnings guided the selection of the research strategy employed in this study. The strategy selection was also influenced by the availability of time and resources to achieve the research objectives. Researchers must not fall into the trap of considering that research strategies are mutually exclusive. For example, a survey strategy may be combined with a case study. Thus, combining research strategies fosters flexibility and enhances the credibility of the findings.

One of the research strategies leveraged in research is the case study. A case study uses multiple sources to investigate a specific contemporary phenomenon within a real-life context empirically. The case study was selected because of the ability to enable the researcher to gain a rich comprehension of the research context and the process (Morris and Wood, 1991, as cited in Saunders, Lewis, & Thornhill, 2009). The strategy also can answer the questions "why," "what," and "how." Yin (2018) emphasizes that a case study is effective in answering the "how" and "why" questions. As a result, a case study is often used in exploratory and explanatory research. In this research, a case study will answer questions such as "How can Information Systems be used to make the cost of BCPs affordable to most large-scale Fortune 500 companies?" and "What can be done to educate large-scale organizations on the cost of risk that they are taking by proceeding without adequate BCPs in place?"

Case Study

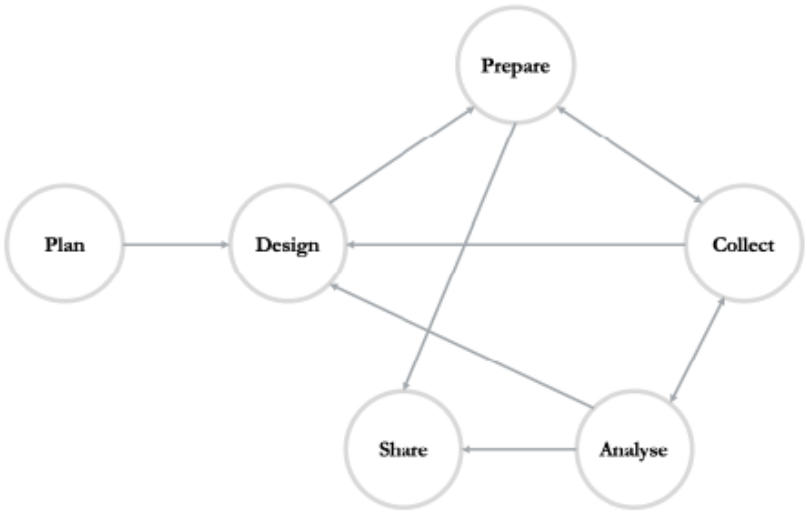
A case study is a vital tool enabling a researcher to examine the problems and solutions implemented by different researchers. Dealing with the findings of other studies also allows the researcher to avoid potential research pitfalls by learning from the mistakes of previous studies (Smith & Albaum, 2012). Case studies are efficient because they comprise histories of other projects and simulations of potential alternatives.

Step 1: Planning the Case Study

Nilsson & Tegström (2020) provides a comprehensive illustration of the research process for case studies. The first step of the process is planning the case study. According to Yin (2018), researchers must follow a rigorous methodological path when conducting research at this stage. Planning for the case study commenced with finding credible sources, followed by a comprehensive literature review. The extensive literature review on the use of systems to create, test, maintain, and execute BCPs was guided by the research questions and objectives. Yin (2018) identified various challenges hindering proper case study research. The challenges include a lack of rigorous research, confusion with non-research case studies, and failure to achieve generalizable conclusions. The challenge of failure to conduct a thorough investigation can be addressed effectively by following systematic procedures and using multiple sources.

The rigor of exploring information systems for business continuity planning in IT-driven organizations was enhanced by following proven and tested scientific techniques backed by sound philosophical underpinnings, including a systematic case study research process.

Figure 12
Research Process for Case Studies



Note. Figure 12 highlights the research process for case studies, including planning, designing, preparing, collecting, analyzing, and sharing the findings (Nilsson & Tegström, 2020).

Step 2: Design

The second step is to develop the research design. The use of information systems to create, deploy, execute, and test BCPs in IT-powered organizations was explored using a case study design. A researcher can conduct single or multiple case studies to achieve the research aim and objectives (Voss et al., 2002; Yin, 2018, as cited in Nilsson & Tegström, 2020). Considering the complexity of using information systems to achieve business continuity and the uniqueness of how companies apply the techniques, multiple case studies are appropriate for this study. Performing various case studies is beneficial because it enhances the chances of drawing generalized conclusions (Voss et al., 2002; Yin, 2018, as cited in Nilsson & Tegström, 2020).

Step 3: Preparing to Collect Data

The third step is to prepare to collect data. According to Yin (2018), the critical considerations in this stage include the suitable skill set, training, and screening of potential case studies. The researcher must have the right skills to conduct case studies. The skillsets leveraged in this study include the ability to ask the right questions, active listening, adaptability, and professionalism when conducting research. Preparing and training for the case studies is also essential. For instance, the researcher was trained in ethics before starting this research. As a result, ethical considerations such as the need to protect the integrity and confidentiality of sensitive data are upheld. The self-sponsored training also ensured a thorough understanding of the methodology and relevant issues to the study.

Step 4: Collect Data

The primary sources of evidence in case studies include documentation, interviews, archival records, and observations. Credible documents were selected for the multiple case studies performed in this study.

Step 5: Analyze the Data Collected

The recommended preparation for performing a case study is to have a precise analytical strategy. The analytical approach gives the researcher rigorous thinking and facilitates linking empirical data with the research questions. Yin (2018) outlines the four general methods for analyzing data. The strategies include relying on theoretical propositions, working with data ground-up, developing case descriptions, and examining plausible rival explanations. The analysis strategy applied in this study is a hybrid of the four designs.

Step 6: Sharing the Findings

The final step in Yin's (2018) proposed process for case studies is to share the results. The report's language and content should be aligned with the intended audience. This study's audience comprises professionals and academicians with relevant knowledge of information systems and business continuity planning, including disaster management and disaster recovery in an IT-driven environment. The audience also consists of groups with unique interests in using information systems to achieve business continuity and the risks of failing to deploy sufficient systems and strategies to achieve business continuity, especially in the context of post-pandemic. The findings of the case studies will be presented in the next chapter. A combination of textual, statistical, and visual information will provide sufficient evidence for the unique readers to conclude.

Case Descriptions

Case A: Business Unit A (BU-A)

The first organization selected for the case study analysis, Business Unit A, specializes in supplying vessel equipment. The company is referred to as BU-A within Case A. BU-A is based in Europe, where Research and Development and Sales operations are based. However, the company has a global network of operations and supply chains (Nilsson & Tegström, 2020). The products and services offered include global sourcing, manufacturing, and supplying vessel equipment. The company's manufacturing sites are in Europe, China, and India, while technical capabilities are based in Asia.

After an extensive literature review, the ideal methodology for this study is case studies. Considering the complexity and the uniqueness of the deployment of information systems to support business continuity planning in IT-driven organizations, the best approach is to use multiple case studies. Numerous case studies will provide a comprehensive outlook vital for answering the research questions. Analyzing various case studies will reveal critical information required to estimate the cost of using information systems to deploy and maintain business continuity systems and the risks of failing to have sufficient BCPs in the context of the COVID-19 pandemic and post-pandemic.

The first section of each analysis briefly describes the case, including the company's details. The first case selected for this study is Business Unit A, referred to as BU-A within the case. The company supplies vessel equipment and operates globally, mainly in Europe, China, and India. According to Nilsson & Tegström (2020), the company's research and development and sales operations are based in Europe, while the critical technology resources and capabilities are in Asia. The Case of BU-A is highly relevant to this

study because the company leverages information systems to support business continuity planning even before the pandemic. Analyzing the effectiveness of the information systems in supporting business continuity planning before the pandemic and post-pandemic provides more insights to answer the research questions and achieve the study's objective.

The business continuity management operations of BU-A are mainly based in the headquarters located in Europe. This is the site housing the company's central processes and functions. After a thorough analysis of the company's business continuity plans, systems, and operations, the following critical points were noted. Firstly, the company integrated business continuity management into its Quality Management System (QMS). The integration of BCM with QMS was based on ISO certification to ensure that action plans are correctly mapped with BCM processes (Nilsson & Tegström, 2020). The integration allows for an annual review to test the systems' effectiveness in enhancing the company's business continuity operations. Mukherjee et al. (2020) offer a divergent view by emphasizing the need to integrate BCP with policies to protect the environment. Therefore, apart from QMS, IT-driven companies should find opportunities to incorporate environmental issues into sustainability BCPS.

Case B: Business Unit B (BU-B)

This section comprehensively describes the case B company in this analysis. Compared to case A company, case B supplies fewer units annually but has a higher value per product. Case B company specializes in technical products that must be configured according to the specific customer needs and used in industrial operations by customers globally. The company's headquarters are in Europe and houses marketing, Research, and Development (R&D) operations, sales, and services. The company has several sites in Europe and Asia. Case B is highly relevant in this study because the company leverages information systems to achieve strategic global and local operations objectives. For instance, the sales department employs more than 25 people specializing in marketing (Nilsson & Tegström, 2020). The company leverages information systems in the sales department to forecast demand and market trends. Information systems are also used to customize products to meet the diverse needs of customers.

In the case of B company, business continuity management and deployment of disaster recovery plans were not significant concerns before the pandemic. However, according to the company's president, BCM processes are implemented at individual sites. Most BCM and BCP processes are conducted independently. The company's executives rely on individual sites to develop and implement customized plans based on standard corporate templates. The top management is only involved in signing off the final BCP plans. They can also challenge individual plans and improve them. The approach implemented by Case B company to review BCP plans concerning quality management systems is consistent with the best practices employed by Case A company.

Case C: Consultative Council for the Americas Central Banks

The third case study provides a more holistic analysis of the business continuity plan and systems based on the scenarios from the Consultative Council of the Americas (CCA) central banks. The pandemic caused unprecedented disruptions in the global supply chain and the use of information technology systems. The implications varied across various industries and companies, especially IT-driven companies. The CCA central banks provide a modernized example of how far IT-driven banks adjusted their business continuity plans to address the issues triggered by the pandemic. The case study of the central banks provides a comprehensive demonstration and illustration of the need to deploy business continuity strategies to enhance resilience in the face of short-term and long-term disruptions.

Limitations of Case Studies

A case study is an experimental inquiry to investigate a contemporary phenomenon in-depth within its real-world context (Yin, 2014, as cited in Glette & Wiig, 2022). A case study enables a researcher to investigate comprehensively by analyzing different cases (Gerring, 2017, as cited in Glette & Wiig, 2022). Despite these benefits, case studies have been criticized as a research methodology that lacks rigor. According to Glette & Wiig (2022), case studies lack systematic procedures and methods that guide the researcher when conducting research. In this study, the lack of rigor problem with case studies was managed by following the recommended steps of executing a case study proposed by Yin (2018). The framework by Yin (2018) provides a systematic and structured procedure for conducting case studies, including preparation, collection, and data analysis.

The second critique of case studies is the lack of generalizability of the findings. Glette & Wiig (2022) assert that case studies lack generalizability, meaning that the results may not be accurately applied in cases other than those studied. However, studies have emphasized that case studies are not designed to develop or generate generalizable data. Case studies are intended to demonstrate the uniqueness of each case. As a result, case studies were embraced in this study to understand the essence of each case regarding implementing information systems to support business continuity plans in IT-driven environments operating in diverse setups. Green et al. (2022) also discussed in-depth how case studies can be used to develop causal inferences between different issues under investigation. Therefore, the capability of case studies to create causal inferences is crucial in understanding the use of information systems to achieve business continuity, including in crisis management and disaster recovery.

Moreover, studies have criticized case studies for the possibility of personal interpretation as bias (Glette & Wiig, 2022, p.1388). Researchers using case studies are vulnerable to discrimination because of the flexibility the interpretivism philosophy allows. In this philosophical stance, the researcher is part and parcel of the research study. The issue was addressed by confining research ethics and ensuring independent analysis and reporting. Multiple studies have been reviewed, and the findings have been compared with those from the case studies. The similar findings and those with contradictory results ensured that this study was free of bias. Consequently, the analysis of the findings of different studies and the incorporation of findings from various studies confirmed that the recommendations of this study are transparent and credible.

Research Ethics

The exploratory study complied with relevant research ethics in each research section. According to Saunders, Lewis, & Thornhill (2009), ethical research practices should be followed in all research stages, including formulation of the research topic, data collection, analysis, and reporting findings. This study complied with the recommended ethical standards and practices in a scientific inquiry, including privacy, confidentiality, consent, and anonymity. The ethical standards of privacy, confidentiality, and anonymity were respected in the data collection step. The names of the companies involved in cases A, B, and C are withdrawn for confidentiality and privacy reasons. Ethical research requires protecting personal and sensitive data in any research inquiry. However, the headquarters' details, primary operations locations, industries, and related data are provided. For instance, the analysis focuses on CCA central banks in case C. The specific details of the banks involved in the data collection are not provided.

The secondary data from previous studies also comply with ethical research standards and practices. For instance, the names of the managers, heads of CRM, CEOs, and employees interviewed or who responded

to the survey are not provided. The participants also signed consent forms before participating voluntarily in the research studies. Incorporating the findings, where consent forms were signed and the names of participants kept confidential, was a strategic effort to ensure this research was executed within the confines of ethical research. The information presented is cited correctly, and the reference list is provided for cross-checking and verification.

The survey used to supplement the findings from the case also complied with the tenets of ethical research. For instance, the participants signed a consent form before participating in the online survey. Only the completed questionnaires within the provided guidelines were analyzed. Implementing such ethical strategies ensured that the study's findings were credible, transparent, and publishable.

Summary

The methodology outlines the procedures for conducting multiple case studies and exploratory studies. The case studies were guided by the principles of interpretivism, inductive approach to research, and exploratory research strategy. The hybrid of findings from the unique information systems cases for business continuity in IT-driven companies satisfactorily answers the research questions and guarantees that the research objectives are achieved.

Results and Findings

Introduction

This chapter presents the findings of Case A, B, and C case studies integrated with JRC's famous "COVID-19: Emergency & Business Continuity" survey. The survey provides accurate information for integration in this multiple case studies analysis. The hybrid of the case studies and survey findings are presented and interpreted with the support of previously published studies in this field. The combination of results provides a solid foundation to answer the primary research questions of this study; using information systems to reduce the cost of BCPs to most large-scale Fortune 500 companies and the risks of failing to deploy adequate BCPs. The findings are analyzed and presented based on their contribution to answering each sub-research question and the five objectives of this study.

Case Studies of Information Systems used by Selected Fortune 500 Companies

Walmart Case Study

Walmart is a multinational retail corporation that operates thousands of stores worldwide. Walmart has implemented various information systems and technologies to support its operations during disruptions to ensure business continuity. Some of the information systems implemented by Walmart for business continuity are:

Supply Chain Management (SCM) System: Walmart's sophisticated SCM system allows it to monitor and manage its supply chain activities in real time. This system provides Walmart with end-to-end visibility of its supply chain and enables it to identify and respond to disruptions quickly. Apart from the SCM, Walmart has implemented several strategies to improve its supply chain and meet the growing customer demand. The company has invested in its supply associates by increasing wages and plans to continue through the holidays. According to Metzger (2021), the company also hired over 3,000 drivers with more permanent supply chain positions to ensure the efficient movement of products through its facilities.

Point of Sale (POS) System: Walmart's POS system is critical to its operations, enabling it to track sales, inventory, and customer behavior in real-time. This system helps Walmart to quickly adjust its inventory levels and manage its supply chain during disruptions. Walmart has increased storage capacity in its

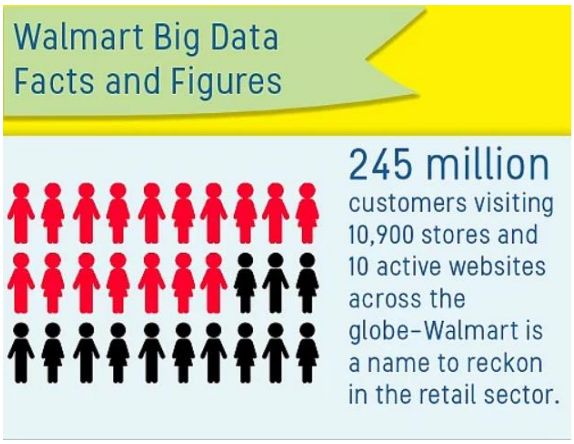
distribution and fulfillment network by constructing new facilities. The company also focuses on enhancing automation capabilities in its existing facilities to facilitate faster product delivery from distribution centers to stores (Metzger, 2021). Walmart is expanding its delivery capabilities and routing online orders directly from its stores.

Electronic Data Interchange (EDI) System: Walmart uses an EDI system to exchange data with suppliers and partners. This system enables Walmart to communicate quickly with its suppliers and partners and adjust its supply chain during disruptions. The information provided by EDI can be used to help some of Walmart's suppliers in several ways. EDI can provide detailed inventory information for each product, enabling suppliers to understand how their products perform at Walmart's stores (Walmart, 2022). EDI can compute sales by location, helping suppliers with market research to identify trends and opportunities for growth. EDI also provides detailed information on product flow, including delivery times and stock levels, which can help suppliers streamline their production and supply chain processes to meet Walmart's demands more efficiently (Walmart, 2022).

Customer Relationship Management (CRM) System: Walmart uses a CRM system to manage customer interactions. This system lets Walmart quickly communicate with its customers and inform them of any disruptions or changes to its operations (Cao, 2022). Walmart's selling strategy is centered around simplicity and cost-savings, and the company strives to remove any obstacles that might prevent customers from making immediate purchases (Cao, 2022). The company's Multichannel initiative offers customers multiple options for purchasing and collecting items, including buying products online through the Walmart App and FedEx sites and then picking them up at the nearest Walmart store (Viktor, 2023). This process is seamless and has no restrictions on purchase and delivery, making it as simple as a banking transaction.

Business Intelligence (BI) System: Walmart's BI system provides real-time analytics and insights into its operations. This system enables Walmart to quickly identify and respond to disruptions and make necessary adjustments to its operations. Walmart's analytics systems can analyze up to 100 million keywords daily to optimize the bidding process for each keyword (Project Pro, 2023). This analysis covers millions of products and hundreds of millions of customers from various sources. By processing this large amount of data, Walmart can optimize its bidding strategy to achieve better results for its advertising campaigns.

Figure 13:



Walmart Big Data
(Project Pro, 2023)

Note. Figure 13 shows a summary of Walmart's Big Data. For instance, 245 million customers visit 10900 stores and ten websites.

Disaster Recovery (DR) System: Walmart's comprehensive DR system enables it to recover from disruptions and resume normal operations quickly. This system includes backup and recovery procedures, redundant systems, and offsite data storage. Among 14 multinational companies representing various industries, Walmart has developed practical approaches to disaster-risk preparedness and response (Cooper, 2013). These companies are part of a collaborative initiative between the public and private sectors, led by the UN Office for Disaster Risk Reduction (UNISDR), to increase global awareness of natural hazards and risk resilience (Cooper, 2013). UNISDR plans to utilize private-sector disaster-management solutions worldwide over the next decade through collaboration with public and private sector entities to create risk-resilient societies worldwide.

Amazon Case Study

Amazon is a global e-commerce and cloud computing company that provides its customers with a wide range of services. Amazon has implemented various information systems and technologies to support its operations during disruptions to ensure business continuity. Some of the information systems implemented by Amazon for business continuity are:

Amazon Web Services (AWS): AWS is a cloud-based computing platform that provides a wide range of services, including data storage, processing, and analytics. AWS is critical to Amazon's operations, enabling it to scale its computing resources quickly during disruptions. AWS Business Continuity Services provides cloud-based backup, disaster recovery, and storage solutions that can be quickly and easily set up without requiring any upfront investment (Amazon AWS, 2023). These services can be purchased as a bundle or on a pay-as-you-go basis, offering companies a flexible and cost-effective way to deal with unexpected situations at any time. With these services, companies can ensure the continuity of their operations in case of disaster or other unforeseen events.

Customer Relationship Management (CRM) System: Amazon uses a CRM system to manage customer interactions. This system enables Amazon to communicate quickly with its customers and inform them of any disruptions or changes to its operations. One of the uses of Amazon's CRM system is providing recommendations to customers based on their past buying behavior. When a user is logged into their account, Amazon recommends several products the customer may be interested in purchasing (Kaur, 2016). This feature is designed to boost sales without pressuring customers. Amazon has also introduced other features, such as the "customer who bought this" feature, which is based on similar buying behavior by other customers, to help customers make informed purchasing decisions (Kaur, 2016). Amazon's CRM system is designed to enhance the customer experience and drive sales through personalized recommendations and targeted marketing.

Supply Chain Management (SCM) System: Amazon's sophisticated SCM system allows it to monitor and manage its supply chain activities in real time. This system provides Amazon with end-to-end visibility of its supply chain and enables it to quickly identify and respond to disruptions (Bharadwaj, 2019). When a customer orders on Amazon.com, the website uses Amazon's order sourcing engine to determine which warehouse should fulfill the order. The decision is made in real-time and is designed to minimize transportation costs associated with the order. Bharadwaj (2019) asserts that by integrating with the order-sourcing engine, the company can quickly and efficiently determine the most cost-effective way to fulfill

the order, whether from a nearby warehouse or a distribution center further away. The system helps Amazon.com minimize shipping costs and provide customers with faster delivery times.

Inventory Management System: Amazon uses an inventory management system to track its inventory levels in real-time. This system helps Amazon to quickly adjust its inventory levels and manage its supply chain during disruptions. According to Polacco & Backes (2018), Amazon has implemented computer-integrated inventory management systems that allow customers to take products off the shelves and leave the store without going through a checkout line. The system is aimed at providing convenience to customers and reducing checkout clerks, which is expected to save costs (Polacco & Backes, 2018). However, the cost of implementing, maintaining, and sustaining the system may offset or exceed the cost-savings achieved by reducing checkout clerks.

Business Intelligence (BI) System: Amazon's BI system provides real-time analytics and insights into its operations. This system enables Amazon to quickly identify and respond to disruptions and make necessary adjustments to its operations. BI is an essential tool for businesses in the modern era, helping them to articulate strategies and make informed decisions based on data. Gupta & Jiwani (2021) emphasize that BI is a decision support system that allows enterprises to analyze data throughout the business process. Machine learning techniques can predict future demand for products or services, enhancing the ability of businesses to plan and make strategic decisions.

Disaster Recovery (DR) System: Amazon's comprehensive DR system enables it to recover from disruptions and resume normal operations quickly. This system includes backup and recovery procedures, redundant systems, and offsite data storage. For instance, Amazon Redshift enables disaster recovery by offering a cross-region snapshot copy feature. The feature allows users to copy their Amazon Redshift cluster snapshots to a different AWS region for disaster recovery (Armenatzoglou et al., 2022). If one part is disrupted or fails, users can quickly and easily restore their clusters in another region without requiring lengthy and complex data recovery processes (Armenatzoglou et al., 2022). The cross-region snapshot copy feature is highly reliable and secure, ensuring that users can quickly and easily recover their data during a disaster.

Apple Inc. Case Study

Apple has implemented several information systems to achieve business continuity. An example is the Apple Business Manager (ABM), a web-based portal allowing organizations to deploy and manage Apple devices and apps at scale. ABM enables organizations to manage their devices and apps remotely, ensuring continuity of operations in the event of disruptions (Apple, 2022). Through ABM, organizations can also remotely wipe devices, enforce passcodes, and set up automatic device enrollment for new devices, which helps to streamline the deployment process.

Apple Business Manager simplifies the process of creating Managed Apple IDs for each user in your organization. These Managed Apple IDs are unique to your organization and can be managed by IT administrators to control access to various services. One of the benefits of Managed Apple IDs is that they are separate from personal Apple IDs, ensuring that company data remains secure (Apple, 2022). Apple Business Manager integrates with your existing environment, so you can provide Managed Apple IDs to employees using their administrative credentials, such as Google Workspace or Microsoft Azure Active Directory (Azure AD).

Apple has also deployed the Apple Device Enrollment Program (DEP), which simplifies the setup and management of devices. DEP streamlines the setup process by allowing organizations to automate the

enrollment process, configure settings, and install apps remotely. This system helps ensure operations continuity by enabling organizations to deploy devices quickly and efficiently, especially during disruptions. Apple Business Manager integrates DEP and Volume Purchasing Program (VPP), along with Mobile Device Management (MDM) software, to enable organizations to manage and deploy Apple devices to their employees quickly (Muema, 2020). With DEP, devices can be automatically enrolled in MDM as soon as activated, making it easy to manage and configure the devices remotely. According to Muema (2020), VPP enables organizations to purchase and distribute apps and books to their employees. These programs and tools simplify the management and distribution of Apple devices in the enterprise setting, supporting business continuity.

Apple also offers the iCloud service, which provides cloud-based storage for documents, photos, and other files. iCloud allows users to access their files from any device, which can help ensure continuity of operations, especially if a device is lost or damaged. iCloud offers automatic backup and restore functionality, which can be invaluable during disruptions, as it helps to ensure that data is not lost or corrupted. Despite the benefits, Apple has encountered various cloud data backup challenges (Menn, 2020). For instance, legal challenges have compelled the company to drop previous plans to improve the backup features of iCloud. Regardless, these information systems implemented by Apple play a crucial role in achieving business continuity by providing organizations with the tools and capabilities to manage devices and data remotely, ensuring that operations can continue in the event of disruptions.

Microsoft Case Study

Microsoft has implemented several information systems to achieve business continuity. An example is Azure Site Recovery, a cloud-based disaster recovery solution that helps organizations protect and recover their data and applications during disruptions (Microsoft, 2023). Azure Site Recovery replicates workloads to a secondary site, allowing organizations to fail over quickly and continue operations without interruption. This system offers automated recovery orchestration, which ensures a smooth and efficient recovery process.

Microsoft has also deployed the System Center Operations Manager (SCOM), an infrastructure monitoring and management system. SCOM enables organizations to monitor the health and performance of their infrastructure and applications, which can help identify issues before they cause disruptions. This system offers real-time monitoring and alerting, which can help organizations to respond quickly to problems and prevent them from becoming significant disruptions (Microsoft, 2023).

Microsoft has also implemented the Office 365 platform, which provides cloud-based productivity and collaboration tools. Office 365 offers cloud-based email, file storage, and collaboration tools, which can help organizations to remain productive during disruptions. The platform is accessible from anywhere with an internet connection, which allows employees to work remotely and collaborate effectively. The software is also used in IoT supply chain and productivity services (Sharma & Dash, 2023). These information systems implemented by Microsoft play a crucial role in achieving business continuity by providing organizations with the tools and capabilities to protect and recover their data and applications during disruptions, monitor their infrastructure, and remain productive and collaborative even in the face of distractions.

Toyota and General Motors Case Study

The supply chain disruptions caused by the COVID-19 pandemic affected the operations of different com-

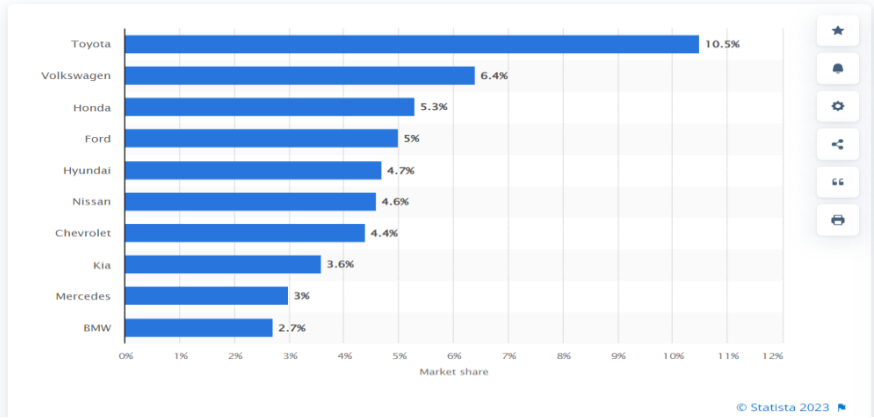
panies globally, including manufacturers. The pandemic significantly impacted the automotive industry, disrupting the global supply chain and decreasing demand for vehicles. Many automakers were forced to halt production and temporarily close their factories to prevent the spread of the virus, resulting in significant revenue losses. The pandemic also caused a shift in consumer behavior, with many people delaying large purchases like cars due to economic uncertainty (Haigh, 2022; Shih, 2022). The pandemic led to a shortage of semiconductor chips used in many modern vehicles, further exacerbating the industry's supply chain issues. As a result, the industry has undergone significant changes since 2022, coupled with other problems, including the increasing pace of electrification and advancements in connectivity technology (Haigh, 2022). These changes are leading to intense competition and challenging existing brand strategies but also present significant opportunities for both established Original Equipment Manufacturers (OEM) and new brands.

Despite the challenges faced by the automotive industry during the COVID-19 pandemic, Toyota outperformed many of its competitors and overtook General Motors as the top seller in North America in 2021 (Carlier, 2022; Haigh, 2022; Shih, 2022). While some observers questioned whether Toyota had abandoned its lean principles of minimal inventories and a pull production system, the company's success during the pandemic highlighted the resilience and adaptability of its production system. Specifically, less understood aspects of Toyota's design, such as its emphasis on flexibility, continuous improvement, and a focus on the long-term, allowed the company to accommodate disruptions better and emerge from the pandemic in a strong position.

In 2021, Toyota emerged as the world's largest motor vehicle manufacturer, with a market share of approximately 10.5 percent, topping the world's largest car brands (Shih, 2022). The Toyota brand is owned by Japan's Toyota Motor Corporation, which surpassed the Volkswagen Group as the largest motor vehicle manufacturer in the world.

Chris Nielsen, Executive Vice President of Toyota North America, attributed the company's success during the pandemic to the Toyota Production System (TPS), stating that "*TPS is really what allowed us to do as well as we did*"(Shih, 2022). Nielsen, who oversaw quality and demand/supply management during the pandemic, worked alongside Jamie Bonini, the President of the Toyota Production System Support Center (TSSC), to manage numerous disruptions. In this article, Nielsen and Bonini provide insights into how TPS has evolved and continues to adapt in a changing world.

Figure 14:



Global Automotive Market Share 2021
(Carlier, 2022)

Note. Figure 14 shows the global automotive market share in 2021 by brand. Toyota topped the market with a 10.5% share, followed by Volkswagen at 6.4%.

The Toyota Production System (TPS) serves as an information system that enables Toyota to achieve business continuity by providing real-time information on all aspects of the production process. By leveraging this system, Toyota can quickly identify and respond to disruptions or problems, allowing the company to maintain operations and avoid costly delays. TPS encourages a culture of continuous improvement and learning, which helps Toyota adapt and innovate in response to changing market conditions and customer demands (Haigh, 2022; Shih, 2022). The system enables the company to remain competitive and achieve long-term success. Ultimately, TPS is a critical component of Toyota's business continuity strategy, helping the company to achieve operational excellence and resilience in the face of disruptions and uncertainty.

The statement by Ted Ogawa, President, and CEO of Toyota Motor North America, highlights the company's appreciation for being included in the Global 500 List. He acknowledges the achievement as a reflection of the hard work and dedication of the global team in providing mobility solutions for customers worldwide (Verlin, 2021). The statement emphasizes Toyota's commitment to excellence and continuous improvement in all aspects of its operations, including developing innovative products and technologies that meet customers' needs while ensuring sustainable growth and development for the company (Verlin, 2022). The statement underscores Toyota's focus on collaboration, teamwork, and customer satisfaction, contributing to its success as a leading global automotive company.

In addition to the TPS, Toyota employs several other systems and practices to achieve business continuity. One is the Toyota Business Practice (TBP), which focuses on improving business processes and decision-making through a structured problem-solving approach. The Toyota Way outlines the company's core values and principles, such as respect for people, continuous improvement, and customer focus (Htun, Maw, & Khaing, 2019). Toyota also strongly emphasizes supply chain management, using just-in-time (JIT) and kaizen to optimize production and minimize waste.

The company has established a global network of suppliers and partners, enabling it to respond to disruptions and maintain business continuity quickly. Toyota's approach to business continuity is based on a combination of systems, practices, and values that prioritize efficiency, flexibility, and continuous improvement (Verlin, 2022).

Toyota competes with General Motors (GM) in several ways, including product development, market share, and operational efficiency. One key competition area is in the development of electric and autonomous vehicles. Both companies have invested heavily in research and development to bring these technologies to market, with Toyota emphasizing its hybrid and fuel cell technology and GM focusing on battery-electric vehicles and autonomous driving technology (Htun, Maw, & Khaing, 2019; Shih, 2022). Toyota has consistently been a leader in the global automotive industry, while GM has historically been strong in the North American market. However, Toyota has been making significant strides in the North American market in recent years, surpassing GM.

Operational efficiency is another area where Toyota competes with GM. Toyota is known for its lean manufacturing techniques and continuous improvement approach, which enables the company to produce high-quality vehicles at a lower cost than many of its competitors. GM has also tried to improve operational efficiency in recent years, but Toyota's expertise in this area gives it a competitive advantage (Shih, 2022; Verlin, 2022). Toyota and GM compete in multiple domains, but Toyota's focus on innovation,

quality, and operational efficiency has helped it remain a leading player in the global automotive industry. As a result, analyzing and comparing the information systems used by the two brands provides more in-depth insights.

Figure 15:

Toyota Increased Sales Statistics

(Wayland, 2021)

Note. Figure 15 highlights the increasing sales of Toyota in 2021 in the US.

GM has implemented several information systems to achieve business continuity. A perfect example is the GM Crisis Management System (CMS), a comprehensive solution for managing crises and disruptions. The CMS monitors events and incidents, allowing GM to assess potential impacts and develop effective response strategies quickly. The system also offers communication tools, enabling GM to coordinate with stakeholders and keep them informed throughout a crisis (Maiorescu, 2016). GM has also implemented the GM Command Center, a centralized operations center that monitors and manages GM's global operations. The Command Center provides real-time monitoring of critical systems and applications, allowing GM to identify and respond to disruptions quickly. The system also enables GM to collaborate with stakeholders across the organization, including suppliers and partners, to ensure a coordinated response. GM's OnStar opened a new command Center in South America in 2022 (Centeno, 2022). The command center enables more personalized and dynamic support for the 24/7 call centers.

GM has also implemented the GM Supplier Business Continuity Program, which helps ensure its suppliers have the resources and capabilities to maintain operations during disruptions. The program includes training and support for suppliers and regular assessments of their business continuity plans and capabilities. During the pandemic, GM developed and implemented an effective business continuity plan (Nair, 2022). These information systems implemented by GM play a critical role in achieving business continuity by providing GM with the tools and capabilities to manage crises and disruptions, monitor and manage its global operations, and ensure the resilience of its supply chain.

IBM Case Study

IBM has implemented several information systems to achieve business continuity. IBM Resiliency Services provides disaster recovery and business continuity solutions to organizations. The Resiliency Services include backup and recovery solutions and cloud-based disaster recovery services, which allow organizations to recover their critical applications and data quickly during a disruption (IBM, 2022). The system also includes automated recovery capabilities, which can help organizations failover their workloads quickly and seamlessly.

IBM has also deployed the IBM Resilient Incident Response Platform, a security incident response platform. The Resilient platform provides real-time monitoring of security events and incidents, allowing organizations to quickly detect and respond to security threats (IBM, 2022). The system also includes communication tools, which enable organizations to collaborate with stakeholders and coordinate response efforts effectively.

IBM has also implemented the IBM Cloud, which provides cloud-based infrastructure and services to organizations. The IBM Cloud offers scalable and resilient infrastructure and a wide range of cloud-based services, such as data storage and analytics, which can help organizations maintain operations during disruptions (IBM, 2022). These information systems implemented by IBM play a crucial role in achieving business continuity by providing organizations with the tools and capabilities to recover their critical applications and data quickly, monitor and respond to security threats, and maintain operations during disruptions through cloud-based infrastructure and services.

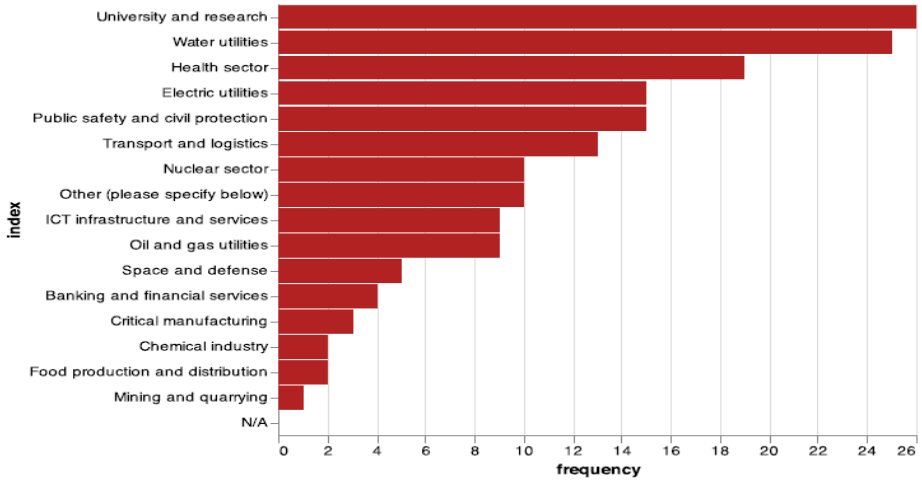
Integrated Findings from Diverse Case Studies and Surveys

The findings are relevant to this study because it involves information from a competitive task force of Critical Infrastructure experts and professionals. The survey was conducted mainly in Europe between April and May 2020 (Galbusera, Cardarilli, & Giannopoulos, 2021). The European Reference Network for Critical Infrastructure Protection (ERNCIP) stakeholders participated in the study. The survey was conducted entirely online via the popular platform referred to as the EU Survey. The members globally were invited to participate in the study via mail listing. Out of the 121 submissions, 118 were correctly completed and considered valid. The survey findings were analyzed based on specific responses for each question.

On top of the case studies, this study leverages the relevant data from this credible survey conducted by a professional and independent international body. The data selected is directly related to the use of information systems in IT-driven organizations to achieve business continuity. A critical analysis of the survey findings shows that most organizations operate in Europe, including France, Austria, Germany, Cyprus, Sweden, Spain, and Finland.

The industry operation for the organizations involved in the study was also crucial for this research. The survey findings show that most organizations operated in the university, research, water utilities, health sector, and electric utilities. In this study, a fundamental assumption is that such industries leverage information systems to achieve business continuity. The findings from organizations are compared with those from cases A, B, and C, which are extensively examined.

Figure 16



In which Sector does your Organization Operate?

Note. Figure 16 shows the frequency of the sectors in which the organizations involved operate. This analysis is vital to this study because it provides insights from experts working in IT-powered environments (Galbusera, Cardarilli, & Giannopoulos, 2021).

The survey also assessed the impact of the pandemic on profitability, demand by clients, and service by suppliers. The findings showed that the pandemic uniquely affected organizations operating in different sectors. The repercussions of the pandemic affected profitability, demand, and supply.

The following revenant ideology derived from the survey findings is the critical dependency for companies in the context of the pandemic. Companies operating in IT-driven business environments work with multiple partners, including service providers and suppliers. The dependencies are essential when developing and implementing systems and strategies to accomplish business continuity in an IT-driven environment. As a result, the findings of this survey are consistent with the case analysis results showing the significance of business continuity systems in industries such as banking.

Figure 17

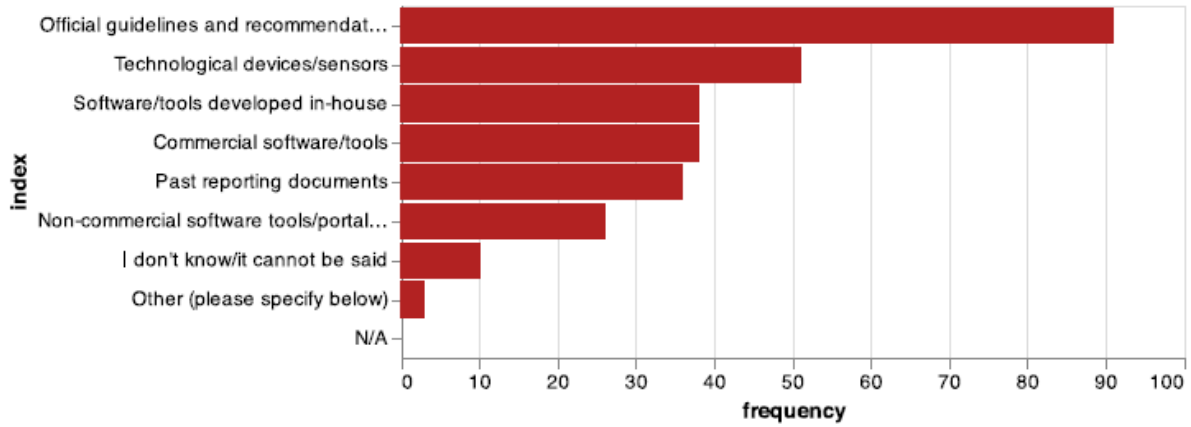
	frequency
Banking and financial services	19 (16.1%)
Chemical industry	16 (13.56%)
Critical manufacturing	19 (16.1%)
Electric utilities	45 (38.14%)
Food production and distribution	7 (5.93%)
Health sector	32 (27.12%)
ICT infrastructure and services	56 (47.46%)
Mining and quarrying	0 (0.0%)
Nuclear sector	7 (5.93%)
Oil and gas utilities	12 (10.17%)
Public safety and civil protection	37 (31.36%)
Space and defense	5 (4.24%)
Transport and logistics	50 (42.37%)
University and research	19 (16.1%)
Water utilities	16 (13.56%)
Other (please specify below)	10 (8.47%)
N/A	1 (0.85%)
total	351 (297.46%)

Critical External Dependencies

Note. Figure 17 shows the critical external dependencies of the companies involved in the survey. The most required external dependencies include ICT infrastructure and services, transport and logistics, electric utilities, and the health sector (Galbusera, Cardarilli, & Giannopoulos, 2021).

The survey also investigated the tools used by organizations for disaster prevention and early warnings. Most of the organizations (80%) used official guidelines and recommendations. However, many organizations also use technological devices, in-house software, and commercial tools to prevent disasters (35-50%).

Figure 18

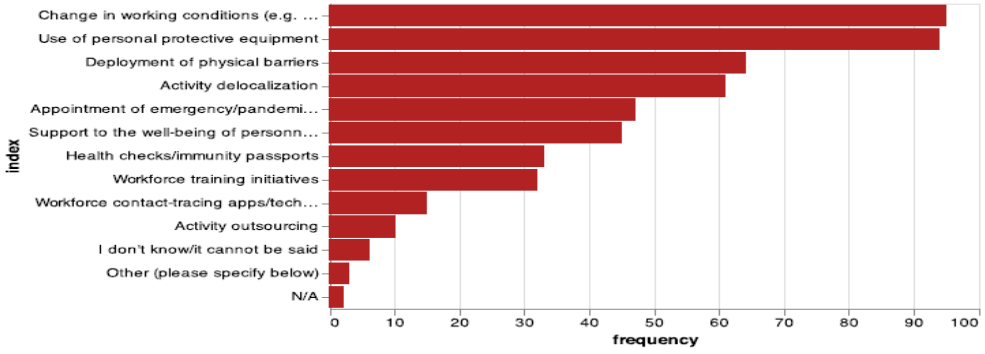


Tools for Disaster Prevention and Early Warnings

Note. Figure 18 shows the tools leveraged by most organizations to prevent disasters at an early stage (Galbusera, Cardarilli, & Giannopoulos, 2021).

The BU-A analysis reveals that disaster recovery planning systems are developed at the site level based on the company's operational BCP templates. These templates outline the minimum requirements for business continuity management and discovery recovery. The possible implications of the disasters on the business are approximated from the top-level perspective. These estimations are regularly reviewed for each product group. Some studies provide a unique recommendation regarding adaptative disaster recovery planning. Adaptive recovery is a unique approach to ensure that business operations resume as soon as possible after a disaster. For instance, managers at the production sites understand the value of faster product delivery and the importance of ensuring operational technology to support the delivery of quality services and products. Risk assessments are carried out regarding sourcing at aggregated product-level and local sites.

Figure 19



Measures to Prepare Recovery

Note. Figure 19 shows the measures for recovery preparation implemented by the different companies. The findings show that most companies implemented changes in working conditions, used personal protective equipment, and deployed physical barriers.

In the case of B, at the product level, the local site manager is responsible for developing BCM plans. However, a key challenge is the lack of a standardized framework. The company only has standardized methodologies for corporate governance policy. A perfect example is the Bravo factory, part of the Case B company. The factory has an efficient local Crisis Management Team (CMT). The team schedules quarterly meetings to revise DRP plans and improve the crisis management procedures and emergency response processes (Nilsson & Tegström, 2020). Though this analysis is not formalized, the company occasionally performs risk analysis centrally within the product groups.

Synthesized Findings Case A, B, and C

The Scope of Disaster Recovery - Case A

The findings show that the institutions involved in case A generally understand what to do during a disaster. However, they lack a structured methodology outlining the procedures and steps recommended to recover or respond to a disaster. The company's plans are integrated with the QMS and mainly focus on on-site infrastructure and information technology (IT). The analysis also revealed that at the product group level, the company's disaster recovery plans focus only on two aspects, manufacturing process, and supply operations (Qi et al., 2021). In manufacturing, the programs address the possibility of critical production equipment failure and provide a guideline for transferring capacity to external suppliers (Nilsson & Tegström, 2020). Regarding the materials supply, the recovery plans mainly recommend backup suppliers in case of disasters.

Furthermore, case A company lacks formalized BCM process. However, the company conducts a "people review" process for succession planning. The people review has played a critical role in improving the company's succession planning by mapping and standardizing succession planning procedures and routines. The findings from Case A are consistent with the results of a study by LeCounte (2020), showing that succession planning for family-owned SMEs is essential for business continuity. The CEOs must integrate succession planning with business continuity strategies to optimize business performance. Though the company lacks a structured BCP, succession planning processes are part of business continuity management. According to case A, managers assess sales manager succession plans regularly (Nilsson & Tegström, 2020).

The Impact of the Pandemic - Case A

The global measures implemented to help curb the spread of Coronavirus had significant implications for the operations of case A company. Actions such as travel restrictions disrupted the company's supply chains and critical manufacturing processes. According to the company, the supply chain disruptions and the implications on digital operations complicated the situation. One product group sourcing manager pointed out that the complexity of certain components impacted more than the cost of raw materials (Nilsson & Tegström, 2020).

For instance, the company closed operations in a critical manufacturing site called Delta in Asia. The issues affecting the availability of information systems affected functions that relied on them. The service technicians also were adversely affected due to travel restrictions and could not access customers to install equipment. Kure & Islam (2019) emphasize implementing strategies to achieve high availability,

confidentiality, and integrity in an IT-powered environment. Fortune 500 companies embrace diverse strategies to achieve high availability and protect data from unauthorized access.

Scope of Disaster Recovery - Case B

The disaster recovery plans for Case B company mainly focus on manufacturing processes and supply of materials. Information systems are leveraged to achieve high precision in metalwork in this company. As a result, production processes are central in disaster recovery planning, especially equipment production. The DRP plans consist of information such as the capacity of each machine, technological capabilities, and identified contingencies to reduce the implications of equipment breakdown and system failure. Due to the complex nature of the product groups and services offered, the technical production capabilities are rarely accessible to external entities. The company has not publicly provided structured processes followed in case of a breakdown. The information on the estimated costs and time to recover from a disaster or system failure is calculated, but the possible payoff analysis by investing in different recovery strategies is not easily accessible. According to the company, maintaining alternative production capabilities is essential for continuity and availability. However, having alternative production capabilities requires constant testing, which is costly.

Regarding the materials supply, disaster recovery plans are developed by the purchasing department at each factory. The DRP consists of a score to measure supply risk and the recommended actions to mitigate it. The score is set using templates based on various factors, including contractual status and supplier performance. The company updates the scores annually in a risk monitoring operation (Nilsson & Tegström, 2020). The company has identified alternative suppliers as a backup plan in some critical components. Though this process is not formalized, each product group takes a coordinated approach to assess risks. Even pre-COVID, the company had already implemented programs to reduce supply chain and information systems risks. However, implementing the risk mitigation strategies such as dual sourcing is expensive.

Top-level risk assessments are conducted through SWOT analysis at the local level companies in the case B company. The unique aspect of case B is that business continuity management is not only limited to infrastructure but has a broad perspective that incorporates the company's people, essential resources, and capabilities. According to the sales manager, the company maps critical resources, such as personnel, with a quality management system but no contingency plans. The company's sales functions are exempted from the BCPs. As a result, there is no structured methodology or procedures on how the company should proceed in case of a disaster affecting the sales functions. Instead, the company relies on experience to deal with risks while working reactively to solve problems as they happen (Nilsson & Tegström, 2020).

The Impact of the Pandemic - Case B

Like company A, the business operations of company B were adversely affected by the pandemic. Most of the procedures were influenced by local government restrictions. As a result, the company's production operations were not adversely affected in countries with lenient limits. As a response strategy, case B company initiated remote working arrangements to enhance the safety of the employees while guaranteeing business continuity during the pandemic. The positive aspect noted is that the transition to remote working was smooth because the company already used digital infrastructure (Nilsson & Tegström, 2020). For example, employees were required to bring their laptops to work, guided by the Bring-Your-Own-Device (BOYD) policy.

The sites in China were closed because of the adverse implications of the pandemic. The company's locations in India were closed temporarily for two months in compliance with government restrictions.

The temporary closure caused delays in processing customer orders and loss of income. Though most of the European sites continued operations, the operations were not to the maximum extent.

Central banks leverage information systems - Case C

Case C analysis is highly relevant to this study because it reflects how central banks leverage information systems to achieve business continuity planning goals and objectives. The case is also appropriate because it involves valuable information from the members of the task force and their diverse experiences addressing the challenges caused by the pandemic and adversely affecting business continuity planning. The insights are valuable in developing and recommending the best practices to enhance resilience against future disasters, especially in a digitally powered business environment (Rosenberg & Tombini, 2022). The best practices are not meant to standardize the process of business continuity planning. However, they should be regarded as general guidance and reference to help organizations identify and effectively solve disasters hindering business operations' continuity.

Before the pandemic, business continuity plans and strategies for most organizations were designed to address interruptions in operations for a short duration, say a few hours or at most one week. The case studies reveal the need for companies to develop business continuity strategies and implement applicable systems that address disasters for long-lasting scenarios. Besides creating BCPs for short-term disruptions in business operations, companies must invest more resources in deploying business continuity plans to address long-term interruptions. Nawari & Ravindran (2019) designed a non-experimental retrospective study to examine the effectiveness of the blockchain in improving post-disaster recovery. Blockchain concepts should be incorporated when developing frameworks to achieve business continuity.

Research Objective 1

To analyze how information systems can help IT-driven companies develop and deploy business continuity plans post-pandemic.

The extensive analysis of Case C set of companies answers this study's research question and objective 1in the following way. The selected central banks leveraged remote working arrangements to enhance business continuity and strengthen operational resilience during the pandemic. The banks implemented four specific activities to improve business continuity and operational stability during the pandemic.

Firstly, the banks invested many resources to ensure employees are connected to the Internet. The banks updated their business continuity plans to empower employees working from home with internet connectivity. Similar arrangements for Internet connectivity were also employed with mobile networks. For example, banks deployed home office resilience programs in which employees were provided with an iPhone and UPS battery, especially those involved in incident management and designated time-critical operations (Rosenberg & Tombini, 2022). The move by the banks to support employees to access the Internet indicates how information systems enhance business continuity in the face of disasters.

Secondly, the company implemented security considerations to enhance the privacy and safety of the employees working from home. Case C analysis reveals that the banks ensured remote employees had access to security protocols and information security policies. Focusing on the security of the Internet for remote working employees ensured that they delivered quality services despite the repercussions of the pandemic. The findings from case C are like the results of a systematic literature review and qualitative content analysis conducted by AlGhamdi et al. (2020) on factors for the successful adoption of information systems. Most information systems governance programs that enhance protection align with organizations' strategic objectives (Bobel et al., 2022). However, to achieve success, top management support is crucial

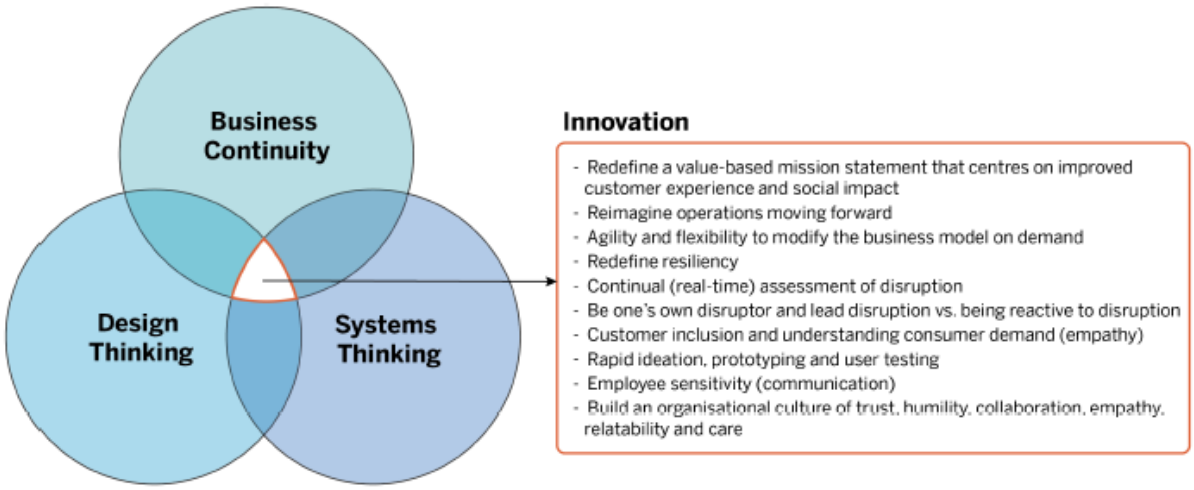
(AlGhamdi et al., 2020). As a result, maximum management support is essential to deploy information systems to achieve business continuity effectively.

Thirdly, the Case C companies implemented tests and exercises to examine and evaluate the effectiveness of the company's critical functions. The banks also tested the efficacy of online collaboration tools, especially during crisis communication. The analysis shows that online collaboration plays a crucial role in enhancing operational resilience and the capability of the company to recover faster from disasters. Based on Case A, senior management did not consider business continuity planning a severe priority. Internal audits recommended that the company improve its Disaster Recovery Planning (DRP). However, there were minimal efforts to follow up and pressure the top management to enhance the DRP systems (Nilsson & Tegström, 2020).

The purchasing managers conduct supplier risk assessments, mainly at the local company levels. The product group sourcing manager conducts inspections at the product group level. The risk assessment's possible implications and findings are escalated to the global sourcing organization when needed. The company's top executives decide whether the risks identified are worth mitigating (Nilsson & Tegström, 2020). For instance, the information from the risk assessment enables the management to decide whether to backup suppliers or implement dual supply strategies.

The hybrid of findings from Cases A, B, and C emphasizes the considerable role of information systems in ensuring that IT-driven organizations achieve business continuity in the face of disasters, attacks, pandemics, and any disruption. Achieving success through information systems requires organizations to understand the intersection and interconnection between business continuity, design thinking, and system thinking. Ivanova (2022) discusses a new agile approach to business continuity. The method is based on the principles of people-centered business continuity.

Figure 20



The intersection of BCP, Design Thinking, and Systems Thinking

Note. Figure 20 shows the intersection between business continuity, design, and systems thinking. For instance, innovation can be achieved through agility and flexibility to adjust business models on demand (Ivanova, 2022).

Finally, the Case C set of banks invested in cross-training as part of the business continuity planning. However, the banks say future cross-training efforts must be more coordinated with the current work-from-home strategy. The commitment of the case C organizations to invest in work-from-home arrangements and the need to secure internet connectivity of employees working from home provides insights into the role of information systems in promoting the creation and execution of BCPs to enhance resilience to future disruptions.

Research Objective 2

To explore the interrelationship between business continuity management, risk management, crisis management, and disaster recovery in a digitally powered environment.

Case analysis C shows a robust connection between business continuity management, risk management, crisis management, and disaster recovery in a digitized banking environment. For instance, the banks have implemented precise security controls to protect and secure different facilities. Rosenberg & Tombini (2022) clarifies that the security controls implemented include confined spacing, call recording, closed circuit television (CCTV), and isolated communication networks. Security controls are critical tools for business continuity planning, but they also enhance the company's operations to manage crises and recover rapidly from disasters.

The analysis also shows that some central banks adopted extraordinary measures to enhance remote employees' security and privacy. The objective of the measures implemented was mainly to ensure that the working environment was safe and conducive. The principle of least privilege, systematic risk reviews, and segregation of duties backed the security controls. Apart from business continuity management, these controls also contribute significantly to enhancing the company's position and readiness to manage future crises. Systematic risk review is a crucial component of crisis management. The combination of such strategies to enhance business continuity shows a close link between business continuity planning, risk management, and disaster recovery in an IT-driven banking environment. A similar case study by Keller, Ollig & Fridgen (2019) shows how top executives such as senior managers, the lead of digital business, and the head of CRM responded to challenges related to business continuity systems. For instance, the head of CRM emphasized building new security systems and mobile apps to secure systems from attacks and threats.

Based on case A, one of the challenges identified is that the company's sales department is not involved in the business continuity management process. The sales manager has not been involved in any training regarding business continuity management. Though the manager is aware of the BCP plans and systems, they cannot access the process or the available documents. The lack of emphasis on the priority of business continuity planning is among the critical reasons for the lack of training and accessibility to BCP plans and information systems within the company.

The hybrid of findings from the case analysis can be better understood and critically analyzed through a comparison with other recently published case studies and reports. Cases A and B provide specific details on how companies adjusted their business continuity plans and systems in response to the pandemic. The challenge identified is that most companies did not have methodological or structured approaches to respond to the disruptions caused by the pandemic. However, Case C provides a more holistic and divergent view of how central banks responded by adjusting their BCPs and systems. Introducing new security protocols and solutions was vital in ensuring banking services were secured and available throughout the pandemic.

World Economic Forum in 2019 recommended a framework for achieving a people-centered future. The first recommendation of the framework is to develop new leadership capabilities to drive innovative people-centered strategies (Ivanova, 2022). The framework also emphasizes the need to manage technology integration in the workplace. According to Ivanova (2022), combining human and automated work enables an organization to achieve optimal performance. The need for new leadership strategies and innovative automation can be maximized to achieve business continuity and prevent future disasters (Aasi, Hajdari, & Yousif, 2020). Therefore, apart from focusing on information systems only, organizations must also consider how innovative leadership strategies can benefit business continuity, crisis management, and disaster recovery post-pandemic.

Electronic Records Management System (ERMS) is an example of an information system successfully deployed to achieve business continuity in the oil and gas industry. Most organizations have deployed new systems, such as ERMS, to replace previous systems for business continuity (Sittig et al., 2014, as cited in Hawash et al., 2020). Protecting information and records from unauthorized access and destruction is part of efforts implemented by companies to achieve business continuity. ERMS enables companies to achieve business continuity by storing documents securely and readily accessible to authorized users. ERMS is considered an effective technology for optimizing the security of records, including sensitive information (Mosweu, 2020, as cited in Hawash et al., 2020).

Figure 21

No.	ERMS benefit
1	Improving an organizations workflow, and providing evidence of business activities
2	Enable automation and monitors records throughout the lifecycle
3	Supporting decision making
4	Enhances records security and integrity
5	Assists in disaster recovery
6	Improving transparency and accountability
7	Eases of sharing information and ease of access to the information during an emergency
8	Provides retrieval history of managing records by tracking all access to records
9	Ensures that only authorized users and administrators can change the content of records
10	Supports and be compatible with the organizational classification scheme
11	Supports for evidence-based policy
12	Supports archives and records management legislation

ERMS, electronic records management system.

Benefits of ERMS

Note. Figure 21 shows the benefits of deploying ERMS to achieve business continuity. ERMS improves organizations' workflow, enables automation, and enhances the security and integrity of records (Hawash et al., 2020, p.37).

Research Objective 3

To examine IT-driven companies' challenges in deploying and executing business continuity and disaster recovery plans.

A thorough analysis of Company B's business continuity plans and systems before the pandemic reveals that different sites attach unique value to BCM and BCP. The company president noted that some

companies are passionate about business continuity planning. Based on the president's sentiments, there has been minimal focus on disaster recovery plans. On the contrary, the company has been heavily concerned with emergency response plans, especially safeguarding employees during disasters.

Based on these revelations, the top management is involved chiefly when making decisions, especially regarding the costs of protecting the company from disasters. For instance, the company's president will be engaged if a specific disaster can affect a production site, leading to a 50% decline in revenue. The top management primarily discusses the costs and funding of the business continuity plans and systems. However, at a strategic level, discussions on investments in contingency plans are rarely discussed. Most of these discussions and decisions are made locally and focus on risk management.

Case C analysis reveals that one of the significant challenges IT-driven companies face in deploying and executing business continuity and disaster recovery plans is the rapid increase in cyber-attacks. Information technology is a critical factor that enabled organizations to migrate operations to remote working during the pandemic. The constant cyber-attacks, including data breaches, hacking, and denial of service attacks, can adversely affect the banking sector's operations. Beyond the pandemic, banks and IT-powered organizations must implement effective measures to address the challenges caused by cyber-attacks.

The analysis revealed that banks plan to introduce new security tools and upgrade the existing ones to enhance security, protection, and detection of attacks and threats. The objective is to prevent successful attacks that may compromise the security of sensitive banking data, including the credit card detail and personal information of the customers. According to Rosenberg & Tombini (2022), some of the security tools that the banks have recommended include network firewalls, anti-spam software, web application firewall (WAF), and hardware security module (HMS). The banking sector also invests in privileged access management (PAM) software and data loss prevention (DLP) tools.

Most organizations have provided their employees with portable computers (laptops) to strengthen remote working as a business continuity strategy. Some companies have also provided employees with licensed software, communication tools, and coordination software. In the banking sector, there is a greater emphasis on multi-factor authentication mechanisms and monitoring remote connections. In similar scenarios, some organizations provide smartphones to all employees to promote remote working arrangements despite cyber-attack challenges. The sentiments are consistent with the recommendations by Koonin (2020) regarding the importance of engaging the local community when implementing BCPs. The Federal Emergency Management Agency (FEMA) is one of the international institutions committed to supporting a "whole community" (Koonin, 2020, p.11). Organizations must leverage the expertise and services of such organizations to improve their business planning and disaster management strategies.

Likewise, the case analysis reveals that IT-powered organizations, especially those operating in the banking sector, are committed to securely securing and empowering their employees to work from home (Sakurai & Murayama, 2019). Introducing new security technologies such as network firewalls, anti-spam software, and web application firewalls indicates that companies are committed to addressing the challenges caused by cyber-attacks and threats to business resilience.

The World Economic Forum framework has a varied view on how challenges related to business continuity should be approached. For instance, in the third recommendation, the framework suggests that the changing complexity and nature of work post-pandemic requires investment in improving employee experience (Ivanova, 2022, p.41). Organizations should also consider building an agile and customized learning culture. Fostering a culture of life-long learning can play a crucial role in addressing the

challenges of using information systems to achieve business continuity. Designing quality products and services also demands organizations leverage the latest technologies (Myerson, 2021, as cited in Ivanova, 2022). For instance, new technologies enable organizations to understand fast-changing customer needs (Hessey & Clarkson, 2013, cited in Ivanova, 2022). Understanding diverse customer needs is vital for business continuity in today's digitized business environment.

Apart from cyber-attacks, the case studies revealed that lack of training hinders information systems' successful development, deployment, and testing from achieving business continuity in a digitized business environment. Staff training emerged as one of the best enablers for the successful deployment of ERMS in the oil and gas industry. According to Hawash et al. (2020), training is vital because it empowers the management and staff with the skills and knowledge required to leverage the new technology. Training employees enables them to understand how to use the latest systems and technologies to execute their tasks and responsibilities. In the specific Case of the ERMS, training programs were designed to facilitate the correct system usage. The training also includes the proper procedures for setting up IT systems and configuring the ERMS to achieve business continuity. The training programs inspire employees and the top management to adopt and accept the ERMS system.

Understanding the cost of training programs enables an organization to estimate the cost of implementing a specific information system to achieve business continuity in an IT-driven environment. In the case of the ERMS system, the cost of implementing technology is depended on various factors, including the vendors, features incorporated in the software, and the necessary software and hardware (Hawash et al., 2020; AlGhamdi, Win & Vlahu-Gjorgievska, 2020). Training the top executives and employees is essential in calculating the cost of information systems to achieve business continuity. The cost of training will also depend on various factors, including the size of the company, the number of employees, and the incentives needed to support the training programs. Hawash et al. (2020) emphasize that quality training is required to ensure employees master the ERMS system and maximize the technology to achieve business continuity. The analysis also revealed no testing or training for discussing disaster recovery within the case B company. The company has no training in disaster recovery planning. When asked about the situation, the president emphasized the company's competence in reaching out to people for support in case of disasters.

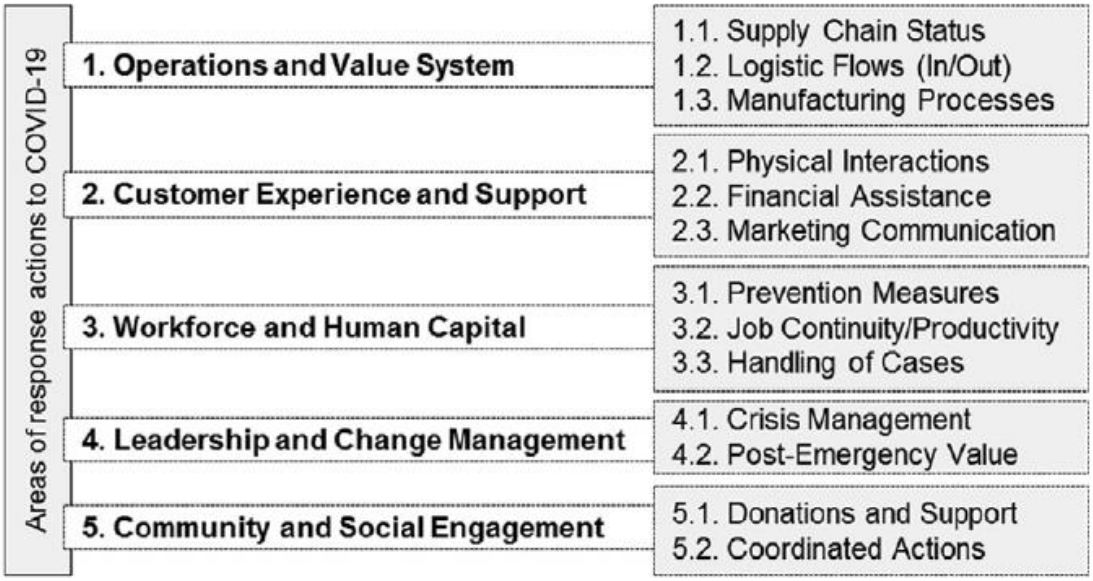
The acceptability of the technology is also a crucial factor that determines the successful deployment of information systems to support a company's business continuity operations and objectives. Many research studies have shown how the acceptance of new technologies is influenced by various factors, including IT knowledge levels and perceptions of the difficulty of learning the latest technology. In specific developing countries, the implementation of Enterprise Resource Planning Software (ERMS) was determined by the user awareness levels and the perception regarding the ease of use (Azima et al., 2019; Rafique et al., 2020, as cited in Hawash et al., 2020, p.39). User satisfaction is also crucial in determining the success of deploying new technology in a digitized business environment.

According to Rasiah, Kaur, & Guptan (2020), implementing information systems to support learning during the pandemic played a vital role in enhancing the continuity of learning. However, the challenges in an online learning environment include poor internet connection and time management skills. Hence, companies must invest in features that promote or support technology acceptability to deploy business continuity systems such as ERMS and ERP successfully.

The framework proposed by Margherita & Heikkilä (2021) explains the key components that should be included in a response strategy based on the lessons learned from the COVID-19 pandemic. The areas of

response action highlighted include operations, value system customer experience, support, and human capital. Human capital measures include preventive measures, job continuity/productivity, and handling cases. The framework also emphasizes the need to incorporate leadership, change management, and social engagement to respond effectively to business challenges.

Figure 22



Response Actions Framework

Note. Figure 22 shows the components of the response actions framework proposed by Margherita & Heikkilä (2021).

The need for competitive IT personnel can never be underestimated in this discussion. Competitive companies relying on technology understand the considerable role of IT personnel and developers in ensuring that systems are up and running correctly. The success rate of implementing information systems such as ERMS depends on the IT personnel's competencies. An organization must have a team of skilled professionals who understand and have passion for the jobs to ensure business continuity. Beyond running smoothly, IT personnel and developers ensure that systems are configured, updated, upgraded, and maintained on the appropriate timelines. Systems and codes must be constantly inspected to verify credibility and prevent any injections that may compromise the integrity of the code. In advocacy countries such as the United States, United Kingdom, and Australia, IT leaders and experts have contributed enormously to the successful deployment of ERMS (Currie & Spyridonidis, 2019; Johare et al., 2013, as cited in Hawash et al., 2020, p.38). These sentiments are also consistent with the oil and gas industry findings indicating IT personnel's role in ensuring the successful implementation of ERMS.

Research Objective 4

To develop a framework to guide the effective use of systems in creating, testing, maintaining, and executing BCPs in IT-driven companies during a crisis or disaster.

A critical aspect that must be considered when developing a framework for effectively using information systems to create, test, maintain, and execute business continuity plans in an IT-driven company is to

analyze the cost. To achieve business continuity and enhance business resilience, a company must estimate the cost of incorporating business continuity planning, crisis management, and disaster recovery planning. Case C analysis provides valuable insights into the cost of supporting remote working arrangements, especially in the banking sector.

In some banks, an economic incentive is provided for remote work exceeding 40% of working time in a week. The support should cover internet and electricity bills and furniture. Some banks have placed a cap of 40% on the time that shall be spent on remote working (Rosenberg & Tombini, 2022). However, this is challenging because most institutions are not subject to such legal provisions. As a result, such companies do not consider the maximum time remote employees are required to work remotely. Some institutions provide a one-off grant for setting up a home office. Once the one-off funding has been provided, the company expects the employee to work remotely successfully. Therefore, case C analysis offers insights into the cost of implementing information systems for business continuity, primarily to support remote working arrangements based on the banking sector scenario.

The case study findings are consistent with the results of a study by Russo et al. (2022). According to Russo et al. (2022), deploying effective and adequate business continuity management systems is demanding, challenging, and time-consuming. Successful implementation of such as system is also a holistic process (Aronis and Stratopoulos, 2016, as cited in Russo et al., 2022). As a result, organizations must invest more in aligning BCPs and strategies to support them. The focus is relevant because it provides insights into how small and medium-sized enterprises can leverage innovative systems to support business continuity. This study focused on large-scale Fortune 500 companies, but the findings from small and medium-scale companies are highly applicable.

According to Russso et al. (2022), when implementing BCMS, strategic guidelines must be developed to guide the process. Besides, to achieve business continuity, the strategic approach must align the systems' goals with the company's objectives. The strategic guidelines will also be crucial in guiding the organization to maximize the specific information system to achieve business continuity effectively (Russo et al., 2022). The analysis revealed how the oil and gas industry maximizes ERMS to achieve business continuity beyond the pandemic. By implementing the ERMS, the IT-driven companies in this sector have enhanced the security and integrity of data, including sensitive customer data. Implementing new security measures in the banking sector also reveals the importance of information security in efforts to achieve business continuity in a digitally powered business environment. As a result, the cost of developing practical strategic guidelines and aligning BCP with BCMS must be considered when estimating the overall cost of using the information to achieve business continuity in an IT-driven organization.

An independent qualitative analysis conducted by Russo et al. (2022) confirms that business continuity training, testing, maintenance, and analysis are some of the less-studied BCM components in the literature. A qualitative synthesis of publications confirmed the statistics. Business continuity plans must be executed and BCP systems configured based on the unique needs of the company (Russo et al., 2022). Fortune 500 companies have striking business continuity, crisis management, and disaster recovery needs. The special conditions are based on various factors, including the company's value proposition, strategic objectives, target markets, and types of information systems deployed. The hybrid of elements must be considered when developing BCPs and strategies to achieve them effectively.

Figure 23

Qualitative Synthesis of Publications

BCM Component	Number of publications
Administration Support and Commitment	48
Understanding the Organisation	31
Risk Assessment	167
Business Impact Analysis	58
BCM Strategy	121
ICT Strategy and alternatives to critical functions	155
BCP Design and Implementation	163
BC Training	20
BCP Testing, Maintenance, and Analysis	68

Note. Figure 23 shows the qualitative synthesis of publications based on the BCM component. Most of the publications focus on risk assessment and the design and implementation of BCP. However, training, testing, maintenance, and analysis of the BCPs are often under-studied (Russo et al., 2022, p. 3).

Research Objective 5

To identify best practices and solutions for empowering digitally powered organizations to leverage business continuity and disaster recovery to increase resilience and sustainability against unforeseen events.

Based on case analysis, an emphasis is on the unprecedented implications of the COVID-19 pandemic and the associated challenges in using information technology systems to achieve business continuity objectives. Organizations have recommended various best practices to enhance resilience against future disruptions (Srivastava, 2020). One of the top recommendations is that organizations must understand the possible implications of risks from different perspectives (Rosenberg & Tombini, 2022). In the case of the banking sector, one of the leading technology-powered sectors, the pandemic's disruptions significantly affected information systems, personnel facilities, and their relationship with the service providers.

The banking sector also faced significant cyber security threats, including ransomware and phishing attacks. According to Phillips & Tanner (2019), the leading cyber-attacks affecting business continuity include phishing, ransomware, and crypto-jacking. Ransomware, for instance, threatens hospitals, government agencies, police departments, and financial institutions (Phillips & Tanner, 2019, p.225). These attacks increased the need to implement more operational risk prevention and mitigation strategies. The fast adoption of remote working arrangements has also accelerated the increase in cases of cybersecurity threats and attacks.

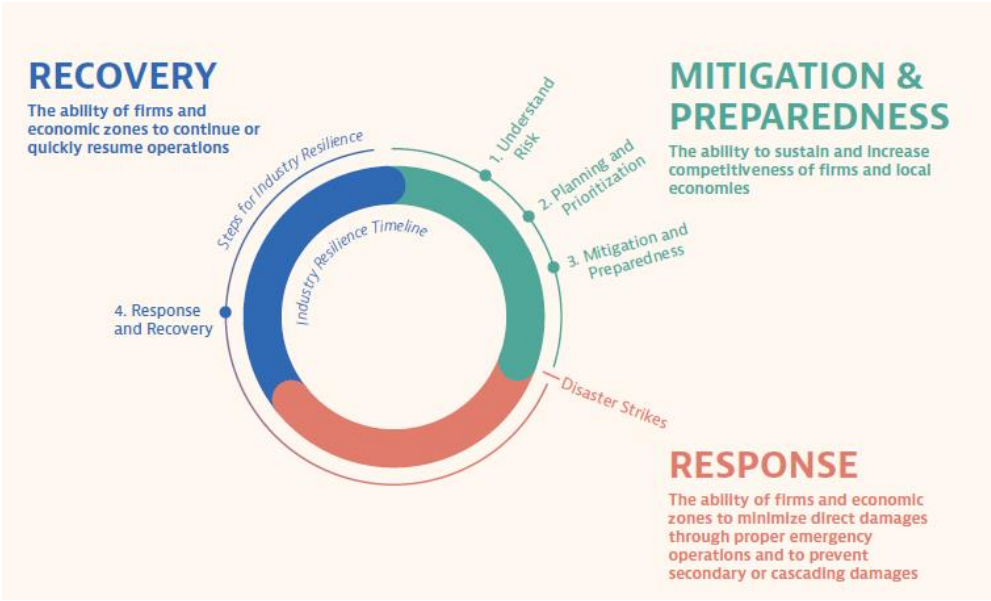
Organizations must invest more time to analyze the risks during and after the pandemic and analyze the effectiveness of the existing procedures to manage risks. Considering the fast evolution of the attacks and threats faced in an IT-driven environment, BCP systems must be upgraded to match these fast-changing needs. The case analysis also emphasizes the need for organizations to spend more resources to mitigate operational risks beyond the pandemic. A semi-structured interview study by Acciarini, Boccardelli, & Vitale (2021) expresses similar but divergent sentiments. For instance, an emphasis is on the need to

develop strategic responses to address business development challenges in the future. Innovative strategies are crucial for mitigating risks that can affect business continuity. However, a company must also consider investing in expertise and information technology tools to manage and enhance resilience to future threats. A recommended best practice is developing a time frame backed by a business impact analysis (BIA). The BIA enables the organization to identify and categorize critical processes and provide valuable information for developing business continuity plans and strategies. Rosenberg & Tombini (2022) assert that BIA focuses on the company's operations and procedures and needs not covered by the contingency plans. The business impact methodology should not be used to facilitate the effectiveness or criticality of the new processes to address the challenges linked to the pandemic. Depending on the business impact analysis outcomes, operational needs, and available resources, a company may determine unique active continuity strategies for significant interruptions.

World Bank (2020) provides a comprehensive case study of the solutions deployed by resilient Japanese industries. It depends on the ability of companies, industrial parks, and sectors to enhance competitiveness. One of the ways it is done is by keeping the company's operations sustained in the face of disasters (World Bank, 2020). The report from the resilient industry in Japan is relevant to this study because it focuses on the solutions and strategies deployed by the manufacturing sector to achieve resilience. Manufacturing is among the industries that leverage information systems to achieve strategic goals and objectives, including processing and packaging.

Figure 24

Resilient Industry: A Timeline of Key Actions



Note. Figure 24 presents a high-level summary of key actions to achieve resilience in Japan's resilient industry. The mitigation and preparedness procedures include understanding risk, planning and prioritization, mitigation, and preparedness (World Bank, 2020, p.3).

The response is the ability of the companies and economic zones to reduce direct damages by implementing effective management operations. Recovery is the ability of companies and economic zones to resume operations quickly after disruption (World Bank, 2020). Response and recovery are crucial to achieving industry resilience, including IT-powered organizations. According to Mukherjee et al. (2020), supporting recovery plans requires the support of service providers, including financial, technical, and

managerial support. Therefore, such factors must be considered when developing a framework to enhance resilience to future disruptions.

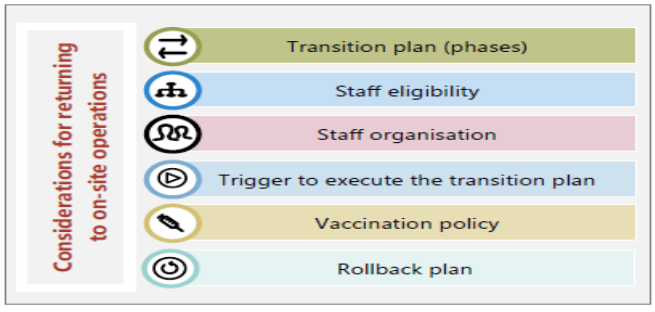
Furthermore, the need to preserve information security has emerged as a critical aspect that must be incorporated into business continuity planning, crisis management, and disaster recovery in a digitally powered business environment (Thakur, Kaur, and Chahal, 2020). Companies, especially in the banking sector, have made tremendous efforts to identify information assets, classify information, and implement applicable security protocols and standards (Rosenberg & Tombini, 2022). Along with these efforts, organizations must continue deploying more innovative security protocols, including DLP tools, to identify better, classify, and protect documents, especially sensitive, personally identifiable information.

The analysis also reveals that to enhance future resilience against future disasters and threats; organizations must consider investing more resources to deploy new tools and solutions, such as hybrid cloud computing, to support business continuity strategies. The transition to a hybrid working scheme where employees work part-time on-site and off-site will continue over the following decades. In the future, most operations and services will migrate to cloud computing and remote working arrangements. These findings are consistent with a study by Modgil et al. (2021), showing that AI-powered supply chains enhance the organizational structure and network resilience. AI enables organizations to leverage data trends, perform simulations, and execute what-if simulations leading to accurate data and understanding of the business environment. Hence, integrating AI into business continuity should be promoted.

Despite the benefits of migrating to a remote working environment, this scheme requires increased resilience to ensure the continuity of operations, especially in an IT-driven climate. Disasters such as social unrest and earthquakes, among others covered extensively in the literature review chapter, can significantly affect the availability of information systems and related services even in a cloud computing environment (Rosenberg & Tombini, 2022). The geographical dispersion of business operations is a critical element of business continuity planning to manage interruptions caused by disasters such as power failure, terrorism, and extreme weather. Companies must consider integrating geographical dispersion strategies to enhance business continuity and cushion operations and systems from unprecedented and unforeseen events. Consequently, considering such factors, an organization must implement a hybrid approach to improve resilience to future disruptions.

Various best practices and procedures have been recommended if a company returns to on-site operations. The task force analyzing the banking institutions involved in Case C developed a practical framework to guide the transition to on-site operations. The framework requires a transition plan, staff eligibility, organization, vaccination policy, and rollback plan.

Figure 25



Framework for On-Site Operations

Note. Figure 25 outlines the considerations for returning to on-site operations in an IT-driven environment (Rosenberg & Tombini, 2022, p.18).

According to Fani & Subriadi (2019), crucial steps must be followed when testing BCP plans and systems. The recommended measures include creating a test mechanism, testing, recording findings, and documenting the testing results. These guidelines will be incorporated into the proposed framework to enhance the testing of information systems for business continuity in IT-driven companies.

Summary

In summary, this chapter presents the case studies' findings integrated with the survey's results relevant to this study. The hybrid of the findings provides sufficient data to satisfactorily answer this study's research questions. The case studies and surveys are compared with the results of previously published studies. The next chapter presents a comprehensive discussion of the findings and the recommended framework for enhancing the use of information systems to support the successful deployment of strategies to promote business continuity in IT-driven companies.

Discussion

Introduction

This chapter presents a comprehensive discussion and explanation of the findings of this study. The chapter is categorized based on the critical themes derived from the results of the systematic reviews and case studies. The key themes discussed in this selection include the main challenges of using information systems to develop, deploy, test, and maintain BCPs and BCMS in an IT-driven company and the proposed solutions. The focus is on the complexity of using information systems to execute BCPs, the lack of tools and resources, and the lack of training and awareness. The chapter also compares the findings of this study with the results of previously published studies related to this research. The information systems for business continuity explored include ERMS used in the oil and gas industry, intelligent BCP automation by Extrasio, Oracle Risk Management Cloud, and Microsoft Azure for disaster recovery.

Using IS to Deploy/Execute BCP/BCM in IT-Driven Companies

The synthesized findings from the case studies and the systematic literature reviews reveal that businesses are vulnerable to disasters. Companies face various hazards that present unique challenges and may develop into catastrophes. However, not every threat grows into a disaster in an organization. The magnitude of disruption caused by hazards and disasters significantly varies. Business continuity planning for sustainability requires a company to understand the potential dangers that may develop into disasters. Case A provided a comprehensive illustration of how an IT-driven company responded to the various risks and disasters affecting the continuity plans and operations. The company's notable strategy is integrating business continuity management into its Quality Management System (QMS). The integration of BCM with QMS was based on ISO certification to ensure that action plans are correctly mapped with BCM processes (Nilsson & Tegström, 2020). The integration allows for an annual review to test the systems' effectiveness in enhancing the company's business continuity operations. However, based on the extensive review and comparison with other company strategies, annual inspections are insufficient to achieve sustainable business continuity, especially in a digitized space. As a result, the starting point of understanding and addressing disasters to achieve business continuity is planning.

The company's regular operations may be adversely affected when hazards develop into disasters. When choosing a site for business operations, it is vital to consider the risks and dangers prevailing in the specific location. Some businesses have ended up severely disrupting business operations for failing to consider

the risks of a particular site. For instance, when developing a business in an area where earthquakes are common such as Tokyo, San Francisco, and Quito, a company must incorporate effective strategies to mitigate earthquake risks (Rundle et al., 2019). Based on the case studies, most companies develop recovery planning systems at the site level. The current practices are based on the company's operations templates for business continuity management. Companies must establish and implement BCPs based on the specific risks prevalent in each business scenario. For instance, the BCPs for businesses operating in disaster-prone regions should differ from those of less risky sites.

Hurricanes and cyclones are among the natural disasters discussed in this study. In several incidences, hurricanes and cyclones have caused massive implications on business operations globally. For instance, Hurricane Maria in Puerto Rico in 2017 affected businesses of all sizes and devastated infrastructure, including roads. According to a study by the Federal Reserve Bank in 2018, Hurricane Maria affected approximately 77% of small-scale businesses (Phillips & Landahl, 2020). These businesses suffered huge losses because of the disruptions and the destruction of utilities. Most companies lacked adequate insurance coverage to address the failures. It emerged that nearly one-third of the businesses affected did not have any insurance coverage at all. The surprising finding is that out of the companies that had insurance coverage, a minute percentage of 6% reported that their claims were met entirely (Hamdni et al., 2018, as cited in Phillips & Landahl, 2020).

Moreover, earthquakes can have devastating implications on business operations, seen and unseen damages which may take a while for the business to identify. Companies must understand that earthquakes can occur globally. However, there are specific places where earthquakes are prevalent (Rundle et al., 2019). Companies must learn from previous incidences of earthquakes to develop effective measures to recover and protect a business from earthquake disruptions. A perfect example is the 2015 Nepal earthquake, which killed almost nine thousand people and threw approximately 3.5 million into homelessness (Phillips & Landahl, 2020). The Nepal earthquake caused up to 10 billion US dollars in economic losses. The implications of the Nepal earthquake highlight the need for support from government and non-government agencies to ensure that businesses survive, especially in the face of natural disasters.

The findings of this study also highlight how volcanoes can have adverse implications on business operations and business continuity plans. The repercussions of volcanoes have been felt, especially in the tourism industry. In 2018, a volcanic eruption adversely affected tourist operations in Hawaii (Meredith et al., 2022). Employers and employees in the tourism industry faced significant losses, including loss of businesses, jobs, and homes (Phillips & Landahl, 2020). Though volcanoes are not prevalent, companies must know that they can cause massive disruptions to business operations. Businesses must conduct regular assessments and analyses to identify areas where such disasters are common.

For example, New Zealand is one of the countries which is home to dozens of volcanic threats. A volcanic eruption may disrupt up to 1.4 million people in the country, leading to a 35.3% decline in the nation's gross domestic product (Phillips & Landahl, 2020). In New Zealand, volcanic eruptions mainly threaten the tourism and manufacturing industries. Businesses operating in volcanic eruption risk areas are vulnerable to high losses that may cost billions, especially when they lack sufficient disaster planning. Mount Zou in Japan is also known for volcanic eruptions. In the past, most businesses in these areas were unaware of the risks and assumed pre-eruption warning messages from the relevant authorities (Donovan, Suppasri, Kuri, & Torayashiki, 2018, as cited in Phillips & Landahl, 2020). Despite the challenges of predicting hazards such as volcanoes and earthquakes, businesses must take seriously the warning system

developed by relevant authorities. Companies must also invest many resources in disaster planning to minimize business disruptions caused by such threats.

This study explored how technological disruptions affect a company's business continuity operations and plans. Companies must rethink how to address technological disruptions affecting business continuity plans. There has been a significant increase in cyber-attacks targeting various business operations and systems. Attacks such as denial of service attacks, ransomware attacks, and phishing attacks can significantly affect the functions of a business (Da-Yu, Hsiao, & Raylin, 2019). A successful denial of service attack can affect critical business operations and services that depend on information systems. A successful denial of service attack can lead to significant downtime and loss of sensitive information, including financial and business records (Aljuhani, 2021).

In 2018, cybercriminals primarily targeted hospitals, causing massive disruptions and threatening the lives of several patients, especially those in Intensive Care Units (ICU). In the United States, for example, hospitals in West Virginia and Ohio had to take serious measures impacting normal operations due to such attacks (Angel, 2022). The successful ransomware attack compromised the hospital's ability to deliver health care, especially in the emergency rooms. Though the impacts were short-term, the successful ransomware attacks ignited discussions on how such threats can affect business continuity operations (Dolezel & McLeod, 2019). Therefore, critical systems such as those used in hospital emergency rooms must be secured from cyber-attacks, including ransomware.

In similar incidents in 2016, cybercriminals attempted to interfere with the US presidential elections through various attacks (Linvill et al., 2019). Federal investigations emphasized the need to implement effective strategies to protect the security and resilience of information systems used for such critical functions. Local and state election systems must be secured to guarantee that their objectives are achieved (Golovchenko et al., 2020; Phillips & Landahl, 2020). The systematic reviews also revealed the significance of space weather as a threat to technology and business operations. Natural calamities have significantly impacted GPS, causing massive implications for cellular services and power grids.

Apart from technological disruptions, the study also reveals the need for implementing dynamic business continuity plans to address contemporary issues such as terrorism and active attacks. International and domestic terrorism can disrupt IT-driven organizations, including schools, universities, and workplaces. Terrorism and active attacks can significantly affect information systems, especially in critical business operations. The rise of cases of mass shootings, especially in the United States, has significant implications for different organizations using information systems to achieve their strategic goals and objectives (Brodeur & Yousaf, 2022). Attacks in Las Vegas and the New Zealand mosque, respectively, in 2017 and 2019, showed different businesses and organizations' increased vulnerability to unprecedented disasters (Phillips & Landahl, 2020).

Cyber intrusions, mass shootings, and ransomware attacks have unique implications for information systems and business continuity plans in an IT-driven business environment. According to Phillips & Landahl (2020), the BCP should ensure normal institutional operations are resumed quickly. Most companies deploy recovery plans but forget to address the psychological implications of disasters on employees. The psychosocial and physical trauma caused by successful attacks should also be incorporated when developing business continuity and recovery plans. In such cases, businesses may need to initiate employee assistance programs to provide guidance and counseling services to employees affected by the implications of the hazard in the workplace (Said & Chiang, 2020; Phillips & Landahl,

2020). The human resource department should address the employees' psychological, physical, and spiritual needs after a disaster.

The COVID-19 pandemic is the most recent disaster that has shown companies in all sectors the need to implement resilient BCPs. The COVID-19 pandemic is not the first challenge faced globally. For instance, the influenza pandemic of 1918 killed more than 50 million people worldwide (Phillips & Landahl, 2020). During the COVID-19 pandemic, companies moved swiftly to implement measures to comply with government and healthcare restrictions to help curb the spread of the Coronavirus (Giunipero, Denslow, & Rynarzewska, 2022). Most businesses and institutions shifted to e-commerce and remote working to ensure business continuity despite the repercussions of the pandemic (Fakieh & Happonen, 2023). The pandemic affected most businesses that did not have business continuity plans and systems.

Despite the significant efforts to develop vaccines to help manage the pandemic, recent studies have shown that the effectiveness of antibiotics and vaccines is still under development. As a result, businesses must prepare better for such pandemics in the future. Integrating innovative strategies such as remote working with BCPs is recommended to enhance the resilience of firms (Fakieh & Happonen, 2023). Business continuity plans and systems should be constantly updated to address such challenges effectively.

The Complexity of Using Information Systems for BCP/BCM

Margherita and Heikkilä's (2021) research showed that only a handful of the Fortune 500 companies surveyed deployed reasonable BCPs during the COVID-19 pandemic. These companies operate in different sectors that rely on information systems and related technologies to achieve strategic goals and objectives. The lack of adequate BCPs in such competitive companies indicates a more challenging situation, especially for small-scale companies leveraging information systems to gain a competitive edge (Margherita & Heikkilä, 2021). This study analyzes and discusses how it focuses on automating the BCM process to enable companies to maximize their benefits through reduced costs. The objective is to find cost-effective information systems methods to create, test, and maintain business continuity plans in an IT-driven business environment.

According to Vogel (2022), BCP can vary considerably depending on a business's unique needs and requirements. Considering the individual needs of IT-driven companies, this study focused on using information systems to create, test, maintain, and execute BCPs. The case studies and the systematic reviews reveal that companies use different information systems to develop, test, support, and implement business continuity plans. One of the most critical issues to consider when using information systems is the security of IS assets (Chapple, Stewart, & Gibson, 2018).

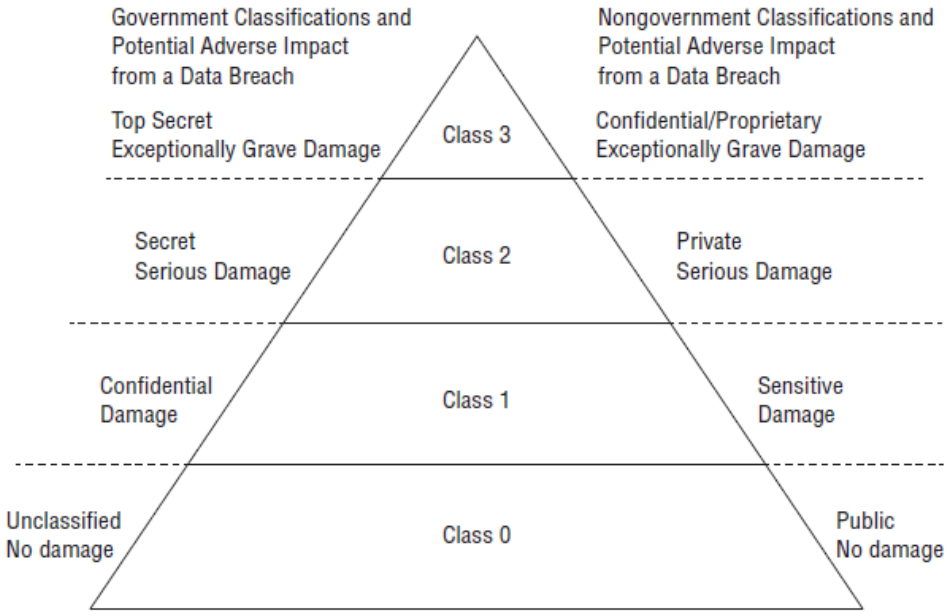
The complexities of using information systems to achieve business continuity are partly linked to underestimating the need for competitive IT personnel. Competitive companies understand the considerable role of IT personnel in ensuring that systems are up and running correctly. The success rate of implementing information systems such as ERMS depends on the IT personnel's competencies. As a result, an IT-driven company must have a team of skilled professionals who understand and have passion for the jobs to ensure business continuity. IT personnel and developers ensure that systems are configured, updated, upgraded, and maintained on the appropriate timelines. They also ensure that systems and codes must be constantly inspected to verify credibility and prevent any injections that may compromise the integrity of the code. In the US, UK, and Australia, enormous contributions are made to ensure the successful deployment of ERMS (Currie & Spyridonidis, 2019; Johare et al., 2013, as cited in Hawash et al., 2020, p.38). Likewise, the oil and gas industry findings indicated that IT personnel played a crucial

role in ensuring the successful implementation of ERMS. Therefore, addressing the complexities of information systems for BCP/BCM requires the organization to engage a multidisciplinary team of professionals.

Securing information systems and assets of an organization is vital in business continuity, especially in the face of disasters. In most organizations, the security policy includes the definition of data classification. It is the responsibility of the IT personnel to tag and secure IS assets as stipulated in the security policy. One of the critical issues that must be included when classifying information is to define sensitive data. Sensitive data is any information that is not meant for the public. Sensitive data may consist of confidential, protected, and proprietary data. Sensitive data must be protected because of business interests and legal compliance necessities. The National Institute of Standards and Technology (NIST) provides a comprehensive definition of personally identifiable information in a special publication titled SP 800-122 (Chapple, Stewart, & Gibson, 2018). According to NIST, PII is any personally identifiable information. PII includes names, SSNs, etc.

Protecting PII drives confidentiality, legal requirements, and legislation globally, especially in North America and Europe. In most organizations, data classification is included in the security policy (Chapple, Stewart, & Gibson, 2018). However, some organizations have separate data policies containing data classification information.

Figure 26



Data Classifications

Note. Figure 26 shows how government data is classified and the potential adverse impact of a data breach. For instance, a data breach on a top secret (class 3) and secret (class 2) has grave damage (Chapple, Stewart, & Gibson, 2018, p.164).

The data security controls deployed by a company play a critical role in determining how the company will respond and recover from disasters. An organization must define how all its data is secured for business continuity. Encryption is one of the best strategies used to enhance data security. Encryption

converts plaintext into scrambled ciphertext, making reading difficult without the decryption key. Chapple, Stewart, & Gibson (2018) assert that leveraging innovative encryption strategies like Advanced Encryption Standard (AES) with 256-bit encryption enables the organization to enhance the security of sensitive data. Combining different encryption algorithms enhances the security of information systems and data.

Furthermore, the case studies revealed that companies are susceptible to attacks and security threats that may adversely affect business continuity plans and systems. A perfect example is the WannaCry ransomware, which significantly impacts hospital business continuity operations (Da-Yu, Hsiao, & Raylin, 2019). The WannaCry ransomware started on May 12th, 2017, and within a short time, it infected at least 300,000 machines spanning over 150 countries (Chapple, Stewart, & Gibson, 2018; Algarni, 2021). Hospitals, large organizations, and public utilities were targeted in this attack. These attacks increase the need for organizations to develop effective measures to enhance data protection and IS security. Besides, it emphasizes the need for organizations to realize the value of their data and have reliable data backups for faster recovery.

Cryptography is an emerging method recommended for adequate and enhanced security for data and information systems. Companies leverage cryptography mainly to achieve 4 inevitable objectives: integrity, confidentiality, non-repudiation, and authentication. However, not all cryptosystems and methods are designed to achieve the four cryptographic goals. Confidentiality ensures that data at rest, in transit, and stored is private. Confidentiality is one of the most cited objectives of cryptosystems, which is to preserve the secrecy of the data stored (Tyagi, Yadav, & Singh, 2021). Symmetric and asymmetric cryptosystems are used to achieve confidentiality. When developing cryptosystems to achieve confidentiality, data at rest, data in motion, and data in use must be considered.

The case studies and review showed how the constant cyber-attacks, including data breaches, hacking, and denial of service attacks, can adversely affect the banking sector's operations. Some security tools the banks have recommended include network firewalls, anti-spam software, web application firewall (WAF), and hardware security module (Rosenberg & Tombin, 2022). The banking sector also invests in privileged access management (PAM) software and data loss prevention (DLP) tools. Hence, combining such security tools and solutions enhances the security of company systems and resilience to attacks and threats.

Integrity focuses on ensuring that unauthorized users do not modify or alter data.

Integrity checks in information systems ensure that the data is appropriately stored and not changed (Tyagi, Yadav, & Singh, 2021). The function of integrity controls is to protect data from any alteration, including intentional deletion, unintentional alteration, and modification by third parties. Authentication validates the claimed identity of system users. Implementing adequate authentication controls in information systems is vital to achieving business continuity. A lack of effective authentication systems and methods may expose data and designs to unauthorized users (Chapple, Stewart, & Gibson, 2018). Unauthorized users may alter the data, affecting its confidentiality, integrity, and organizational value.

On the contrary, non-repudiation assures that the message was sent from the legitimate sender. Wallace & Webber (2017) notes that non-repudiation ensures that no one else is masquerading as the sender of the message received. Therefore, when using information systems to achieve business continuity, it is vital to incorporate confidentiality, integrity, authentication, and non-repudiation controls.

An extensive review shows that most companies plan for external risks, such as pandemics and natural hazards, to maintain business continuity. The challenge is that most companies fail to adequately prepare for the continuity of the information systems and related technologies used in an IT-driven business

environment. Companies must understand that information and data systems are vulnerable to cybersecurity threats and attacks that may adversely affect business operations (Wallace & Webber, 2017). Data system risks must be incorporated in BCPs because they can have adverse implications on multiple organizational departments. Data and information systems share expensive hardware such as networks, file servers, and central computer systems.

These findings are consistent with a study by Argaw et al. (2020), showing that cybersecurity attacks can have adverse implications on sensitive hospital operations. Various systems determine the magnitude of risks of the organization's data systems by multiple factors, including the architecture of the data systems and information systems.

The Critical Process Impact Matrix is a tool used to assess and examine data and information system risks in an IT-driven business environment (Wallace & Webber, 2017). In the systems column, the organization enters the name commonly called the computer system, such as the materials management system. Enter information about the computer in the platform column, such as the database server and firewall name.

The time and days when the program is needed are indicated in the regular operating days. For instance, if the system must always be on, enter 24 hours. Enter the hours or days for the critical system to run in the crucial operating days/time column. In the support primary/backup column, enter the name of the specific IT personnel responsible, not a public entity such as the helpdesk (Wallace & Webber, 2017). For the customer contacts and primary/backup, specify the IT personnel's name to convey upcoming system or current system problems. Mostly the references of the department manager are provided in this column.

The lack of standardized systems and procedures also hinders companies from implementing innovative solutions such as regular backs to achieve resiliency. Some companies have efficient local crisis management teams, so backup can be vital when responding to disasters, especially those affecting information systems. A team is limited because meetings to revise DRP plans and improve the crisis management procedures and emergency response processes are scheduled occasionally. However, backups are automated and require minimal input from the employees. Argaw et al. (2020) recommend training, awareness, and patch management to address the challenges linked to cybersecurity threats in an organization. Companies must learn from the implications of previous incidents, such as the WannaCry ransomware, to develop and implement effective solutions to achieve business continuity and resilience.

The Lack of Tools and Resources

The extensive analysis shows that businesses lack the tools and resources to effectively respond and manage disasters that can affect business continuity plans and operations, especially in a digitized business environment. The starting point of this discussion is understanding the different types of disaster plans that can be leveraged in an IT-driven business environment. Businesses must use different disaster planning strategies to prepare effectively for disruptions, minimize potential risks, and maximize the available tools and resources for each stage (Phillips & Landahl, 2020).

Mitigation planning takes place before the event or disaster occurs. Mitigation planning aims to reduce the potential implications of a catastrophe on human lives, property, and business operations. Mitigation plans must include specific actions recommended for the key stakeholders, including the management, employees, and customers. However, a company must identify potential hazards before planning and conducting a risk assessment. The emergency manager must collaborate with the planning team to review and determine each risk's frequency and potential impacts. These sentiments are related to the findings of a systematic review study by Raikes et al. (2019) showing how a lack of mitigation planning and

preparedness planning affected businesses operating in areas prone to disasters such as droughts and floods. The systematic review focused on 147 articles on mitigation and preparedness planning in developed countries prone to floods and droughts (Raikes et al., 2019). The case studies showed that business continuity management and deployment of disaster recovery plans were not significant concerns before the pandemic in most companies.

In most companies, BCM processes are implemented at individual sites. Most BCM and BCP processes are conducted independently. Businesses must conduct risk assessments at each business site. Based on the findings, they must identify and prioritize the related risks to ensure that resources are allocated effectively. Prioritizing the risks enables the emergency manager and the planning team to make accurate decisions on deploying countermeasures. For instance, strategies may include preventative measures such as concrete posts to prevent the implications of hazards such as poor driving. Non-structural mitigation strategies include buying insurance and complying with building codes and regulations.

The next type of planning vital in business continuity is preparedness planning. Preparedness planning involves different activities, including training employees and creating environments for them to practice. Practicing includes workshops and conferences to test and exercise disaster plans. Professionals must be involved in preparedness planning. For example, professionals will craft a message to convey to different stakeholders regarding the threats identified, including the employees and the public. Semi-structured telephone interviews conducted by Houston et al. (2019) revealed the significant role played by the US media in disaster preparedness and communication. Besides reporting disasters, journalists create content to foster preparedness, mitigation, and long-term recovery and resilience (Houston et al., 2019). The case studies showed that some IT-driven companies have disaster recovery plans. The DRP plans consist of information such as the capacity of each machine, technological capabilities, and identified contingencies to reduce the implications of equipment breakdown and system failure. Employees must be trained to use such technologies to minimize breakdowns and human error.

Similarly, response planning is vital in the modern workplace to achieve business continuity. Mitigation and preparedness plans are useless if the organization has no response plans (Nawari & Ravindran, 2019). In most disasters, the first responders are the employees and the neighborhood. These critical people must be trained to respond effectively to potential disasters. Businesses must learn from incidents by conducting active attacker training. Employees should also be exposed to first aid classes to equip them with better response strategies during emergencies.

The case studies also showed that some companies understand how to respond to a disaster. Most IT-driven companies have no structured methodology with specific response and recovery strategies. The challenge is that BCPs are integrated with QMS. As a result, there is a need to develop more effective and practical tools and resources that enable a business to accurately address disasters and risks that may affect business continuity. A non-experimental retrospective-prospective study by Nawari & Ravindran (2019) shares similar sentiments, highlighting how blockchain technologies can be integrated with BIM to enhance the post-disaster rebuilding process. The combination of BIM and blockchain concepts enhances recovery and rebuilding, especially in an IT-powered environment.

Most businesses today do not understand the importance of response planning. Response planning is primarily leveraged in healthcare organizations considering the vulnerability of such organizations to emergencies. From the 2018 active attacker shooting incident in Las Vegas to recent disasters, it is proven that people are vital in responding to disasters and emergencies (Phillips & Landahl, 2020). Even in cases where there is minimal training, the first responders are essential in addressing and managing the risks.

The objective of BCP here is to make sure that the first responders, especially the employees, are equipped with the skills and knowledge to respond effectively to any disaster the company may face. The objective is to save lives and property before the appropriate authorities respond.

Finally, recovery planning is crucial in business continuity planning. The recovery period depends on different factors, including the company's size and the attack type. An IT-driven company's recovery period from an earthquake differs from that during ransomware or denial of service attacks. The direct implications of the attack on critical business functions also influence the recovery. The impact of the specific threat on the vital assets and systems of the enterprise also plays a crucial role in determining the recovery. New technologies like blockchain should be integrated with business continuity systems to achieve recovery and resilience post-disasters (Nawari & Ravindran, 2019). Having a solid recovery plan can have a significant impact on the time taken by an organization to respond and recover from disasters. The case studies also highlighted how most executives rely on individual sites to develop and implement customized plans based on standard corporate templates. The top management is only involved in signing off the final BCP plans. They can also challenge individual plans and improve them (Röglinger et al., 2022). The top management must actively develop all the tools and resources required to achieve business continuity, including mitigation and recovery plans (Phillips & Landahl, 2020; Nawari & Ravindran, 2019). The lack of a standardized framework for structuring the BCM process and reviewing BCP plans also emerged as a concern in most IT-driven companies examined in this study. Consequently, developing standardized frameworks, tools, and resources will enable the business to achieve business continuity and sustainability.

The focus of recovery planning is to provide guidelines and a road map for the organization to follow to recover from a specific threat or attack. An effective business continuity or recovery plan must outline the specific roles of groups involved in the recovery process. The program must also outline the necessary actions that must be taken to ensure that the operations of the business resume normalcy within a reasonable amount of time (Houston et al., 2019; Nawari & Ravindran, 2019). For instance, the urgency of recovery may differ in a healthcare facility compared to a learning institution. Regardless of the industry, the recovery plan must ensure that continuity of operations is achieved within the shortest time possible.

Lack of Training and Awareness

Training on BCP/BCM Automation

The case studies and systematic review showed that lack of training and awareness is also a challenge hindering the successful development, deployment, testing, and maintenance of BCP/BCMs in an IT-driven company. Companies must invest in training and awareness programs to ensure employees and executives have the appropriate skills and competencies to leverage information systems to achieve business continuity. Businesses must expose their employees to the latest technologies for automating BCP/BCM, including those that leverage artificial intelligence and machine learning (Mao, Zhang, & Tang, 2021). The employees must also be exposed to various use cases of these technologies to understand the challenges solved and the benefits of each system.

Russo et al. (2022) argue that deploying effective and adequate business continuity management systems is demanding, challenging, and time-consuming. Successful implementation of such as system is also a holistic process (Aronis and Stratopoulos, 2016, as cited in Russo et al., 2022). As a result, organizations must invest more in aligning BCPs and strategies to support them. The acceptance of new technologies is influenced by various factors, including IT knowledge levels and perceptions of the difficulty of learning

the latest technology. The implementation of ERMS was determined by the user awareness levels and the perception of ease of use (Azima et al., 2019; Rafique et al., 2020, as cited in Hawash et al., 2020).

A perfect example of new technology that leverages AI to automate business continuity planning management was recently launched by Xtrasio. Extrasio is one of the leading technology companies offering automation of business continuity planning. The company believes in making things easier for customers by leveraging bespoke, secure, intelligent, and optimal AI-based automation solutions. Extrasio's specialized domain involves pioneering novel opportunities across diverse business sectors and consumer applications by quickly deploying cutting-edge technologies such as Intelligent Bots, Automated Data Synthesis, Automated Business Continuity Planning & Management, and Enhanced Decision-making (Extrasio, 2022a).

The company offers an intelligent BCP automation platform providing organizations with a visual representation of their entire Business Continuity Plan, including a timeline-based view and mapping of various stages and entities. The platform offers comprehensive BIA and Risk Assessment capabilities, allowing for the creation of Incident Management and Business Continuity plans (Extrasio, 2022a). Procedures can be invoked by notifying employees with just one click. The workflows are fully automated, user-friendly, and easily customizable to suit the organization's needs.

Most companies in this study relied on templates outlining the minimum requirements for business continuity management and discovery recovery. The possible implications of the disasters on the business were approximated from the top-level perspective. Though these estimations are regularly reviewed for each product group, most companies lack formalized BCM process. The intelligent software offered by Extransio can address such challenges by ensuring that companies have access to the visual representation of BCPs, especially on a timely basis. The software automates most processes leading to faster and more accurate planning and enhancing the business's capabilities to respond to and manage disasters and risks.

The case studies showed that the lack of emphasis on the priority of business continuity planning is among the critical reasons for the lack of training and accessibility to BCP plans and information systems within the company. Electronic Records Management System (ERMS) is an example of an information system successfully deployed to achieve business continuity in the oil and gas industry. ERMS enables companies to achieve business continuity by storing documents securely and readily accessible to authorized users. ERMS is considered an effective technology for optimizing the security of records, including sensitive information (Mosweu, 2020, as cited in Hawash et al., 2020). Despite the benefits, such technologies can achieve minimal results if the organization fails to invest in training and awareness programs. IT-driven companies must invest in training to ensure employees master using systems like ERMS to achieve business continuity and resilience.

Intelligent BCP Automation Use Case in IT Services

Most organizations examined in this study have provided their employees with laptops to strengthen remote working as a business continuity strategy. Companies have also provided employees with licensed software, communication tools, and coordination software. In the banking sector, there is a greater emphasis on multi-factor authentication mechanisms and monitoring remote connections. However, lack of training hinders information systems' successful development, deployment, and testing from achieving business continuity in a digitized business environment. In the oil and gas industry, staff training emerged as one of the best enablers for the successful deployment of ERMS. According to Hawash et al. (2020), training is vital because it empowers the management and staff with the skills and knowledge required to

leverage the new technology. In the case of automation software such as those offered by Extrasio and Oracle, employee training is crucial to achieving tangible results.

Nevertheless, to overcome the challenges in the IT industry, Extrasio deployed iBoTs to automate the processes and services across various business verticals. Voice engineering applications were also implemented to enhance the automation process. These solutions have significantly reduced the time to complete IT Service Desk requests while streamlining the implementation of the Infrastructure-As-A-Service (IAAS) paradigm across the company (Extrasio, 2022b). The intelligent Email response handler has further improved the efficiency of customer support operations, while voice support widgets have enhanced the overall customer experience. Ultimately, these solutions have ensured the smooth functioning of critical business operations.

Companies must invest adequate resources to ensure employees are thoroughly trained on new technologies for business continuity. Training equips employees with the skills and knowledge to use the technologies correctly. Based on the case studies, ERMS training programs were designed to facilitate the correct system usage. The training also includes the proper procedures for setting up IT systems and configuring the ERMS to achieve business continuity. The organization must understand that such training programs are crucial in inspiring technology acceptance.

Figure 27

Benefits of Automating BCP in IT Services

Note. Figure 27 highlights the IT industry's benefits of automating BCP/BCM (Extrasio, 2022).

In IT-driven companies, automating Business Continuity Planning (BCP) using information systems has become crucial to ensuring the smooth functioning of critical business operations. Automation can significantly reduce the time taken to complete tasks, streamline the execution of complex infrastructure management processes, and improve the efficiency of customer support operations. Using iBoTs and other automated systems, IT-driven companies can automate tasks such as IT service desk requests, email and chat support services, and 24x7 service request monitoring (Extrasio, 2022b). Deploying these automated systems can optimize execution time, eliminate dependency on SMEs, and ensure the uninterrupted functioning of critical business operations.

In some companies, maintaining alternative production capabilities emerged as a strategy essential for continuity and availability. However, having alternative production capabilities requires constant testing, which is costly. Though BCPs incorporate the company's people, essential resources, and abilities, many companies still need help to achieve the best out of their systems, especially those designed for business continuity and management. Based on the use cases of the IT services and the banking sector, the need for automating Business Continuity Plans (BCPs) in an IT-driven company should never be underestimated.

Automation of BCPs can help organizations handle complex processes, reduce dependency on SMEs, and ensure business service continuity and availability (Extrasio, 2022b; Extrasio, 2022c). It can also provide real-time visibility into the health of the IT environment, enable the automation of UI, Web & CLI-based activities, and unify monitoring consoles to view all applications from a single window. Additionally, automation can reduce the overall execution time of processes, provide end-to-end monitoring of jobs, and ensure adherence to BCP compliance and audit reports.

Oracle Risk Management Cloud

Oracle's Risk Management Cloud is like the intelligent systems offered by Extrasio but designed uniquely to address diverse challenges related to business continuity in an IT-driven business environment. Oracle's Risk Management Cloud offers companies a digital solution to automate risk management and business continuity workflows. The solution prepares companies for unexpected situations and ensures business continuity through up-to-date plans, readiness surveys, issue identification, and resolution proposals (Oracle, 2023). The solution also allows for assessing, updating, and certifying existing business continuity plans.

In addition to digitizing risk and continuity workflows, the Risk Management Cloud by Oracle provides real-time risk analysis, risk mitigation strategies, and automatic risk detection capabilities. The platform also allows for creating and customizing business continuity plans and automating plan activation and response. The solution can identify potential risks using predictive analytics and offer recommendations for mitigation strategies (Oracle, 2023). Furthermore, the platform provides a centralized repository for all risk and continuity-related data, making it easily accessible and searchable for analysis and reporting purposes. Oracle's Risk Management Cloud delivers a comprehensive, flexible solution for managing risk and ensuring business continuity.

Information Systems for Resilient BCPs/BCM

The Need for Resilience

Companies have the potential to achieve resiliency by leveraging information systems to automate business continuity planning and management. Organizations have received recommendations to swiftly respond to potential operational failures and contagion risks both internally and externally (De Preter, 2021). Practical solutions have relied on deploying nimble business procedures, requiring redesigning or modifying current operations and utilizing digital tools as critical enablers. Most companies have been compelled to depend on their existing resources to confront and surmount the emergency (Margherita & Heikkilä, 2021). Effective reactions have, therefore, also relied on the presence of technical reserves that are useful in maintaining the continuity of operations during the transition phase and facilitating seamless adaptation of the organization to the evolving business environment.

Based on the findings from the ERMS system, a company operating in an IT-driven business environment must invest in innovative information systems for business continuity. The cost of implementing a strategy is depended on various factors, including the vendors, features, and the necessary software and hardware (Hawash et al., 2020). The cost of training employees must be included when calculating the cost of information systems to achieve business continuity. The cost of training will also depend on factors such as the number of employees and the incentives needed to support the training programs. Hawash et al. (2020) emphasize that quality training is required to ensure employees master the ERMS system for

sustainable business continuity. Acceptability also determines the successful deployment of information systems to support a company's business continuity and resilience.

Organizations have established an up-to-the-minute comprehension of the pandemic's consequences via advanced data collection and monitoring abilities. Effective reactions have been founded on implementing successful business analytics techniques and tools that promote information-laden communication and leadership (Margherita & Heikkilä, 2021). These findings emphasize the importance of leveraging information systems to execute successful business continuity plans (BCPs) in response to the pandemic. The actions include developing immediate reactions, relying on crisis management capabilities and technical reserves, and adopting effective business analytics methods and tools to support information-rich communication and leadership.

The use of information systems, such as advanced data gathering and monitoring capabilities, has allowed organizations to gain real-time awareness of the pandemic's impact and make informed decisions accordingly. Margherita and Heikkilä (2021) emphasize that adopting digital technologies as key enablers has enabled implementing of agile business processes and redesigning or modifying current operations. Effective communication and leadership, supported by business analytics methods and tools, have been critical to ensuring the sustainability of operations during the transition phase and facilitating seamless adaptation to the changing business situation. Thus, leveraging information systems is crucial for organizations to execute BCPs successfully and navigate the challenges of the pandemic.

Network Security for Resilient BCPs

The network is crucial for business continuity in an IT-driven business environment. The network has specific security concerns that need to be addressed, primarily focused on physical security. Access to the network closets and freestanding cabinets should only be granted to authorized personnel, and the network administrator must collaborate with the facility's security manager to ensure the doors are always locked. Additional vents may be added to the entries based on the closet's airflow (Wallace & Webber, 2017). It is essential to limit the number of people who hold keys to the cupboards and cabinets by using sub-master keys, which must be carefully tracked. If a key is lost, the locks may need to be rekeyed. Therefore, minimizing access to the network closets and cabinets is crucial to ensuring the network's security.

Another crucial area to consider is logical security, which involves password protection for network software on servers and devices. These passwords should be kept confidential and known only to authorized network support staff. However, they should also be written down and stored in the Data Processing Manager's office in case the key staff members are unavailable. An acceptable use policy should prohibit anyone from plugging privately-owned devices into the network to prevent unauthorized access, including contract employees (Wallace & Webber, 2017). This policy should also extend to connecting to wireless nodes to prevent unauthorized access and network disruption. Implementing these measures ensures that the network's logical security is robust and protected from unauthorized access.

Servers are critical network infrastructure components that support multiple users and essential host applications. Losing a server can significantly impact business operations, so it is vital to have processes in place to facilitate server restoration. According to Wallace & Webber (2017), two ways to ease server restoration are storing backup tapes and software off-site and standardizing hardware, software, and peripherals. Keeping backup videos and software off-site ensures that they are protected in the event of a disaster, while standardizing hardware, software, and peripherals can simplify the restoration process by

reducing the complexity of the server environment. By adopting these measures, the network can minimize the impact of server failures and ensure business continuity.

A critical aspect of network management is documentation. Keeping the physical and logical network diagrams up to date is essential, as they are crucial for restoring the network after a disaster. The physical diagram should illustrate the facility's layout and the primary cable routing, while the logical chart should show the network nodes and their interconnections. By documenting both graphs, the network can ensure efficient restoration in case of a disaster. Another crucial documentation is vendor information (Wallace & Webber, 2017). Maintaining up-to-date hardware, software, and peripheral vendor information can simplify the restoration process. The network can minimize downtime and ensure business continuity by keeping accurate documentation.

Finally, collaboration with the security team is crucial for maintaining system security and minimizing the risk of data loss due to security breaches. By working with the security team, the network can implement appropriate security measures to protect against potential threats. In an emergency, the network must be able to configure new servers while maintaining the latest level of security (Wallace & Webber, 2017). The security team should be involved in planning to guide security measures that must be considered during disaster recovery. By collaborating with the security team, the network can reduce the risk of security breaches and maintain the system's security level during recovery.

On-Premises to Azure Disaster Recovery

Risk factors and their potential impact on an organization are often overlooked, which is why an enterprise risk management team can be helpful. These individuals are responsible for closely monitoring and identifying potential risks. Before designing or implementing plans, IT and non-IT organizations should examine common risk areas (Chakraborty & Chowdhury, 2020). Risk assessment is critical when undertaking business continuity and disaster recovery planning. By identifying potential risks, organizations can better prepare for and mitigate the impact of any unforeseen events that may occur.

There is a misconception that having an off-site backup solution is enough to protect your data and ensure disaster recovery compliance. However, backing up data on or off-site does not guarantee complete protection or the ability to recover data in the event of a single point of failure. The cloud can help by providing a copy of the data in a different location, allowing recovery operations to begin while the primary site is down (Chakraborty & Chowdhury, 2020). To truly protect an environment against any downtime, it is essential to have both a comprehensive backup and disaster recovery strategy in place.

Figure 28

Risk Classification	Risk Examples
Disaster risk	Storm, tsunami, earthquake
Financial risk	Delayed payment, credit ratings, currency devaluation
Human resource risk	Employee misconduct, labor disputes, workplace accidents and injuries
Market risk	Fierce competitor movement or failure of new product introduction
Environmental risk	Disease, fires, contamination, and leaks
Distribution risk	Transportation carrier failure
Security risk	Terrorism and workplace security
Regulatory risk	Regulatory change or government policy change
Operational risk	Demand uncertainty, poor delivery, poor planning, bad customer service
Safety risk	Workplace accidents and injuries
Supplier risk	Supplier performance failure, rising material costs
IT risk	Failure of software systems or loss of important data

Recovery Site Common Risks

Note. Figure 28 shows the common risks in recovery sites. The hazards include disaster, financial, human resource, market, security, and IT risks (Chakraborty & Chowdhury, 2020).

Microsoft ASR is an ideal solution for customers who require a coordinated approach to failover that utilizes various geographical locations and enables controlled failover between them. This product offers a single Disaster Recovery solution operating across Hyper-V, VMware, and physical infrastructure platforms. Besides, it supports a variety of cloud environments, including public, private, and service provider clouds (Chakraborty & Chowdhury, 2020). ASR enables users to achieve their desired Recovery Time Objective (RTO) and Recovery Point Objective (RPO) by using a range of communication channels.

The Role of External Parties in BCPs

The Federal Emergency Management Agency (FEMA) provides post-disaster assistance in the United States and administers the National Flood Insurance Program (NFIP). FEMA has established procedures to prevent financial waste from fraudulent claims and aid recipient fraud (Kushma, 2022). However, their ability to effectively implement these procedures has been questioned following recent large-scale disasters. Other agencies also aid affected individuals, and there are limitations to data sharing across programs and agencies.

FEMA provides post-disaster assistance through the Public Assistance Program, the Individuals and Households Program, and Hazard Mitigation Grant Program. The Individuals and Households Program, Hazard Mitigation Grant Program, and National Flood Insurance Program (NFIP) directly help individuals and families, while the Public Assistance program helps communities (Kushma, 2022). All these programs have provisions for risk reduction and can be used to fund hazard mitigation activities. However, in some cases, individuals may be required to apply for a loan from the Small Business Administration (SBA) instead of receiving a direct grant.

A disaster's impact can disrupt the operations and continuity of organizations and businesses, necessitating new measures and procedures for recovery. Hurricane Ike's impact on Houston, Texas, highlighted the importance of several strategies, including strengthening organizational capacity, promoting collaboration across sectors, providing swift financial support, and involving non-profit organizations in pre-disaster planning and mitigation efforts (Kushma, 2022). Similarly, Rider emphasized the significance of incorporating disaster services into routine services and organizational structures to develop standard and adaptive expertise, reduce conflicts, and prioritize services effectively.

Effective long-term recovery after a disaster necessitates a thorough and holistic approach involving many stakeholders. It must also be guided by a clear vision and supported by the political will to implement measures that safeguard communities from future hazards and increase their resilience. As the operating environment becomes more intricate and harder to navigate, the need for adaptability and innovation becomes even more challenging.

Learning from disasters should be a cumulative process that builds on the lessons of previous events rather than being defined solely by the most recent significant catastrophe. Arendt highlighted the importance of community leaders engaging in interactive planning throughout the recovery process and adjusting plans based on feedback and other information (Kushma, 2022). This adaptive planning approach enables stakeholders to address obstacles and unintended consequences and celebrate incremental progress toward recovery, even when victories are small.

Cost of IS for Creating, Deploying, Testing, and Executing BCPs

The cost of implementing information systems for business continuity, such as those used by Walmart, can vary widely depending on the size and complexity of the organization, the number of techniques and technologies required, and the level of customization and integration needed. However, it is essential to note that while there is a high upfront cost to implement these systems, the investment is typically justified by their benefits, such as increased efficiency, enhanced resilience, and improved customer satisfaction (Data Foundry, 2019). Some costs associated with implementing information systems for business continuity include hardware, software, integration, and maintenance.

According to Shi & Veres (2021), the type of system maintenance includes corrective maintenance (CM), preventive maintenance (PM), and failure-finding maintenance (FFM). CM is conducted after system failures, while PM is executed to prevent future failures. FFM incorporates functional and operational diagnosis of the system (Shi & Veres, 2021). An organization should allocate sufficient resources for the execution of the different system maintenance activities.

The cost of acquiring and installing the necessary hardware and software, such as servers, network equipment, and licensed software applications, vary based on the systems. In some situations, companies have exploited unique ways to achieve tradeoffs between the effectiveness and cost of information systems for business continuity. In a study by Soufi, Torabi, & Sahebjamnia (2019), the soft business continuity plan selection (SBCPS) model was leveraged to achieve tradeoffs between the resilience of BCPs and the implementation costs.

Customizing and integrating the systems and technologies to meet the organization's specific needs is also costly. The cost is high when integration requires additional programming, configuration, or data integration work. In custom software development, the size and complexity of an application, along with its creative design and integration with other systems, are significant factors that influence its cost. Small applications typically have 10-25 screens; medium-sized ones have 25-40 screens and complex applications have more than 40 screens (Data Foundry, 2019). Complicated logic, heavy analysis, scoring, and number crunching can increase the time needed for coding and testing, increasing the cost. The more extravagant the creative design needs, the more expensive the costs (Data Foundry, 2019). Integrating with external software can introduce unknown variables, and the ease or difficulty of integration varies depending on the integrated system.

Personnel, maintenance, and support costs: The cost of hiring and training personnel to manage and maintain the systems, including IT staff, business analysts, and project managers. The ongoing cost of maintaining and supporting the systems, including software updates, hardware maintenance, and technical support, must be considered when evaluating the cost-effectiveness of these systems (Shi & Veres, 2021; Haseeb, 2019). The cost of implementing information systems for business continuity can range from tens of thousands to millions of dollars, depending on the scope and complexity of the project (Data Foundry, 2019). However, these costs are often justified by the benefits of these systems' increased resilience, efficiency, and customer satisfaction.

Figure 29: Average Cost of Downtime

Availability	Hours downtime per year	Cost per hour* (small company)	**Total annual downtime risk**	Cost per hour** (average company)	**Total annual downtime risk**
98%	174.74	$16,920	**$2,956,601**	$531,060	**$92,797,424**
99%	87.36	$16,920	**$1,478,131**	$531,060	**$46,393,402**
99.5%	43.68	$16,920	**$739,066**	$531,060	**$23,196,701**
99.9%	8.736	$16,920	**$147,813**	$531,060	**$4,639,340**

Note. Figure 29 shows the average cost of downtime per hour and annually. For instance, the average cost of downtime per hour is $531,060 for a medium company (98% availability) (Data Foundry, 2019).

Challenges of Using IS to Create, Implement, Test, and Execute BCPs

The implementation of information systems is crucial for achieving business continuity. However, these systems come with challenges that organizations need to address. The high cost of implementing these systems can hinder adoption for smaller organizations with limited budgets. A survey conducted by Haseeb et al. (2019) revealed that SMEs struggled to adopt new technologies in Thailand due to a lack of resources. Lack of sufficient resources, including adequate funds, can hinder the successful deployment of information systems for business continuity (Gqoboka, Anakpo, & Mishi, 2022). Companies' technical issues when implementing new technology include data management and the organization's functional structure (Haseeb, 2019). The technical complexity of these systems can be challenging, requiring specialized skills and knowledge to implement and maintain them. Integrating these systems with legacy systems can also be problematic and may require additional investments in integration technologies.

Other challenges of these systems include the risk of security breaches, dependence on technology, and the possibility of system failure. Organizations must invest in robust security measures to protect their systems and data from cyber threats. Overreliance on technology can make organizations vulnerable during disruptions, especially when systems fail, resulting in downtime and loss of productivity (Data Foundry, 2019). Therefore, organizations need to invest in redundancy and backup systems to mitigate the risk of system failure. Addressing these challenges can help organizations achieve business continuity and ensure their operations remain resilient during disruptions.

While the information systems implemented by Apple for business continuity offer several benefits, they also come with several challenges. A crucial challenge is a cost of implementing and maintaining these systems, which can be high for smaller organizations with limited budgets. The high price can be a barrier to adoption for some organizations, especially those that may not have the resources to invest in these systems. The sentiments are consistent with a survey by Haseeb et al. (2019) showing how SMEs struggle to implement new strategies because of resource deficiencies. As a result, companies must invest adequate funds to ensure that systems deployment to achieve business continuity are successful.

The technical complexity of these systems may require specialized skills and knowledge to implement and maintain. Additional training costs and specialized personnel may be required. Moreover, integrating these systems with legacy systems can be challenging and may require other investments in integration technologies. Besides, these systems store and transmit sensitive data, making them vulnerable to security breaches. Tawalbeh et al. (2020) provide a comprehensive discussion of how security threats and attacks such as DDoS can adversely affect the successful operations of IoT. The multiplicity of data collection in an IoT environment increases vulnerability to security threats, including authentication challenges

(Tawalbeh et al., 2020). Organizations must invest in robust security measures to protect their systems and data from cyber threats, which can be costly to implement and maintain.

Finally, organizations that rely heavily on these systems may become too dependent on technology, making them vulnerable during disruptions. The issue can result in downtime and loss of productivity, which can significantly impact the organization (Data Foundry, 2019; Haseeb, 2019). Therefore, organizations need to invest in redundancy and backup systems to mitigate the risk of system failure.

Conclusion and Recommendations

Conclusion

The conclusion highlights the purpose, methods, essential findings, and insights from the discussion of the results of the case studies. The drivers for business continuity and the cost of implementing information systems to accomplish business continuity during disruptions and disasters are highlighted. The findings of the case studies, including the challenges of the information systems leveraged by Fortune 500 companies, are leveraged to formulate evidence-based recommendations. The recommended strategies for educating organizations on the risks of continuing operations without sufficient BCPs are presented. The conclusion and recommendations show how information systems can be used to make the cost of BCPs affordable for most Fortune 500 companies.

Effective business continuity management (BCM) capabilities have become paramount as businesses become increasingly interconnected and reliant on complex systems. In today's dynamic and unpredictable business environment, organizations face many natural and artificial business interruptions that can significantly impact their operations, reputation, and financial performance (Phillips & Landahl, 2020). Consequently, companies must develop effective BCM capabilities to minimize the impact of disruptions and quickly resume normal operations.

The first driver of the need for BCM capabilities is the rise in natural and artificial business interruptions. Natural disasters, such as earthquakes, hurricanes, floods, and artificial disruptions, such as cyber-attacks, terrorism, and supply chain disruptions, can cause significant interruptions to businesses (Krell, 2006; Brodeur & Yousaf, 2022). These events can result in the loss of critical infrastructure, data, and resources, causing business downtime, revenue loss, and damage to reputation (Rostek, Wiśniewski, & Skomra, 2022). Thus, organizations need robust BCM capabilities to mitigate the impact of such events and ensure business continuity.

The second driver of the need for BCM capabilities is the growing impact of business interruptions on organizations due to rising business interconnectivity. As businesses become interconnected, disruptions can be felt across entire supply chains and ecosystems, leading to significant economic and reputational damage (Phillips & Landahl, 2020; Niemimaa et al., 2019). In today's global business environment, where businesses rely on multiple suppliers and partners to deliver products and services, disruptions in one part of the chain can cause a ripple effect that impacts the entire ecosystem (Krell, 2006). Thus, effective BCM capabilities are critical to ensuring the whole ecosystem's resilience and minimizing disruptions' impact on business operations.

Likewise, there are two more reasons why the need for effective Business Continuity Management (BCM) capabilities is increasing. One is the essential obligation for organizations to protect, preserve, and build value. Organizations are responsible to their stakeholders, including customers, employees, shareholders, and the broader community, to ensure their operations are resilient to disruptions (Krell, 2006). The failure to prepare for and respond to disruptions can result in a loss of trust, reputation damage, and financial

losses. Thus, building effective BCM capabilities is essential to protect and preserve the organization's value.

Moreover, the increasing need for effective BCM capabilities is the emergence of new regulations and guidelines on BCM. Regulators and standard-setting bodies, recognizing the importance of BCM, have introduced new rules and guidelines that require organizations to establish BCM programs to ensure they are adequately prepared for disruptions (Margherita & Heikkilä, 2021; Krell, 2006). For example, ISO 22301 is a standard that provides a framework for BCM and sets out requirements for implementing, maintaining, and improving BCM programs (ISO, 2022). Compliance with such regulations and guidelines is not only a legal obligation but also a business imperative. It can help organizations demonstrate their commitment to resilience and enhance their reputation.

To meet these obligations and prepare for potential disruptions, organizations must take a proactive approach to BCM. The procedure involves identifying potential risks and vulnerabilities, developing comprehensive BCM plans, and regularly reviewing and updating them. Effective BCM planning requires the involvement of all stakeholders, including employees, customers, suppliers, and partners, to ensure a coordinated response in the event of a disruption. Organizations must also invest the necessary resources to develop and implement effective BCM capabilities (Shih, 2022; Phillips & Landahl, 2020). The process entails allocating budgets, hiring qualified personnel, and leveraging technology to enhance resilience. Effective BCM requires a culture of resilience and preparedness, which must be fostered throughout the organization, from top management to front-line employees.

The need for effective BCM capabilities continues to increase due to the essential obligation to protect, preserve and build value, and new regulations and guidelines emerge. Organizations must take a proactive approach to BCM and invest the necessary resources to develop and implement effective BCM capabilities. A comprehensive and coordinated effort involving all stakeholders and fostering a culture of resilience and preparedness is needed (Krell, 2006; Margherita & Heikkilä, 2021). Organizations must take a comprehensive approach that includes risk assessment, contingency planning, crisis management, and communication strategies. A deep understanding of the business, its dependencies, and the potential impact of disruptions is necessary. BCM planning must be aligned with the organization's strategic goals and be integrated into its risk management strategy. BCM plans must be regularly reviewed, tested, and updated to ensure their effectiveness in the face of changing threats and risks.

The need for effective BCM capabilities has become increasingly important in today's dynamic and interconnected business environment. As the number of natural and artificial disruptions continues to rise and the impact of interferences increase, organizations must invest in robust BCM capabilities to ensure business continuity, protect their reputation, and minimize financial losses (Aljuhani, 2021; Da-Yu, Hsiao, & Raylin, 2019). A comprehensive approach that includes risk assessment, contingency planning, crisis management, and communication strategies is required. These approaches must be regularly reviewed, tested, and updated to ensure effectiveness.

Recommendations for using IS to make the Cost of BCPs Affordable

Recommendation 1: Adopt Cloud-Based Solutions

Organizations can consider adopting cloud-based solutions to reduce the cost of BCPs. Cloud-based solutions provide scalable and cost-effective infrastructure, reducing the need for expensive hardware and infrastructure investments. According to Kutame et al. (2021), cloud-based systems offer cost-effective BCM and allow flexible and sustainable operations. Cloud-based solutions can also provide easy access

to critical applications and data during a crisis, enabling organizations to maintain operations without needing expensive disaster recovery infrastructure.

Cloud-based solutions can help to make the cost of Business Continuity Plans (BCPs) more affordable for Fortune 500 companies by providing scalable and cost-effective infrastructure. For example, Amazon Web Services (AWS) offers a wide range of cloud-based services, including disaster recovery and backup solutions, enabling organizations to recover critical applications and data quickly during a disruption (Amazon AWS, 2023). AWS also provides scalable and cost-effective infrastructure, reducing the need for expensive hardware and infrastructure investments. For instance, Amazon Quick Sight enables customers to ask questions and use machine learning to identify patterns (Dzulhikam & Rana, 2022). Thus, it allows organizations to maintain operations during a disruption without needing expensive disaster recovery infrastructure.

Microsoft Azure provides cloud-based disaster recovery solutions that enable organizations to quickly recover their critical applications and data during a disruption. Azure also offers a range of cloud-based services, such as data storage and analytics, which can help organizations maintain operations during disruptions without needing expensive hardware investments. Microsoft Azure Stream analyses service leverages a global metadata system to perform real-time analytics (Dzulhikam & Rana, 2022). Therefore, this can significantly reduce the cost of BCPs for organizations, as they no longer need to invest in costly infrastructure and hardware to ensure business continuity.

Cloud-based solutions can help to make the cost of BCPs more affordable for Fortune 500 companies by providing scalable and cost-effective infrastructure, reducing the need for expensive hardware investments, and enabling organizations to maintain operations during disruptions (Dzulhikam & Rana, 2022; Amazon, 2023). By adopting cloud-based solutions, organizations can ensure that their BCPs are effective and affordable, allowing them to recover quickly during a crisis.

Recommendation 2: Automation

Automation can be leveraged to reduce the cost of BCPs. Automating routine tasks and processes can reduce the need for manual intervention and lower the costs associated with staffing and maintenance. Automated testing and recovery procedures can also reduce the time and cost associated with testing and validating recovery plans. Robotic Process Automation (RPA) is an example of automation technology for automating business processes for enhanced continuity and sustainability (Siderska, 2021). RPA combines artificial intelligence and machine learning techniques to automate business processes and operations. Siderska argues that disruptive technology has been implemented successfully, enabling a business to cut costs, maximize resources and save time. Consequently, innovative companies, including large-scale Fortune 500 companies, should leverage such technologies to automate BCPs and repetitive business operations.

Automation can help make the cost of Business Continuity Plans (BCPs) more affordable for Fortune 500 companies by reducing manual labor and human error, which can lead to costly mistakes and prolonged downtime during a crisis or disaster. For example, Walmart uses automation to ensure the continuity of its business operations during disruptions (Raina, 2022). It uses automated inventory tracking and replenishment systems to provide critical products that are always available to customers, even during supply chain disruptions. As a result, it reduces manual intervention and enables Walmart to maintain its operations during a crisis.

General Motors uses automation to ensure the continuity of its manufacturing operations during disruptions. It uses automated robots and equipment to produce its vehicles, reducing the need for manual

labor and ensuring that its manufacturing operations can continue even during a labor shortage or disruption (Siderska, 2021). The technology reduces the cost of BCPs for General Motors by providing it can maintain its functions during a disruption without incurring expensive labor costs.

Automation can help make the cost of BCPs more affordable for companies by reducing manual labor and human error, which can lead to costly mistakes and prolonged downtime during a crisis or disaster (Esquivel-Vargas et al., 2019). By adopting automation solutions, organizations can ensure that their BCPs are effective and affordable, enabling them to recover quickly during an emergency or disruption while minimizing the associated costs.

Recommendation 3: Virtualization

Virtualization can reduce the cost of BCPs by enabling organizations to consolidate their infrastructure and reduce the need for expensive hardware investments. Virtualization provides faster recovery times and reduces hardware maintenance and support costs. Virtualization can make the cost of Business Continuity Plans (BCPs) more affordable for Fortune 500 companies by reducing the need for physical infrastructure and hardware, which can be expensive to maintain and scale. For example, IBM uses virtualization to ensure the continuity of its business operations during disruptions (IBM, 2022). It uses virtual servers and cloud-based infrastructure to run critical applications and data, reducing the need for physical hardware and infrastructure investments. Therefore, it reduces the cost of BCPs for IBM by eliminating the need for expensive hardware and infrastructure investments while ensuring it can maintain its operations during a crisis.

Virtualization can help make BCPs more affordable for companies by reducing the need for physical infrastructure and hardware, which can be expensive to maintain and scale (Salhab, Rahim, & Langar, 2020). By adopting virtualization solutions, organizations can ensure that their BCPs are effective and affordable, enabling them to recover quickly during a crisis or disruption while minimizing the associated costs.

Recommendation 4: Risk Assessment

Conducting a thorough risk assessment can help organizations identify and prioritize critical applications and data, enabling them to focus their investments on the most vital areas. Review can help to reduce the cost of BCPs by ensuring that resources are focused on the most critical areas and reducing the need for expensive investments in non-critical areas. Risk assessment can make the cost of Business Continuity Plans (BCPs) more affordable for Fortune 500 companies by enabling them to prioritize their investments based on their risk exposure and potential impact on the business. For example, Amazon uses risk assessment to ensure the continuity of its business operations during disruptions (Amazon, 2023; Grondys et al., 2021). It identifies critical systems and applications and assesses their risk exposure to various threats and vulnerabilities. The solution helps Amazon prioritize its investments in BCPs and protect its critical systems while minimizing unnecessary investments.

Microsoft leverages risk assessment to ensure the continuity of its business operations during disruptions. It assesses the risk exposure of its supply chain and identifies critical suppliers and components. The solution enables Microsoft to prioritize its investments in BCPs and ensure its supply chain is resilient to disruptions while minimizing the associated costs (Microsoft, 2023).

Risk assessment can help make the cost of BCPs more affordable for companies by enabling them to prioritize their investments based on their risk exposure and potential impact on the business (Rezaei Soufi, Torabi & Sahebjamnia, 2019). By adopting risk assessment solutions, organizations can ensure that their

BCPs are effective and affordable, enabling them to recover quickly during a crisis or disruption while minimizing the associated costs.

Recommendation 5: Standardization

Standardizing BCPs across the organization can help reduce the cost of BCPs by reducing the need for customized solutions and the cost of maintenance and support. Standardization can also help to ensure that recovery plans are consistent and effective across the organization (Apple, 2022). Standardization can make the cost of Business Continuity Plans (BCPs) more affordable for Fortune 500 companies by enabling them to streamline their processes and reduce complexity. By standardizing their processes and systems, organizations can reduce the need for custom solutions and minimize the associated costs. For example, Walmart uses standardization to ensure the continuity of its business operations during disruptions (Walmart, 2022). The company has standardized its supply chain processes and systems, enabling it to respond to disruptions and minimize the associated costs quickly and effectively.

Apple uses standardization to ensure the continuity of its business operations during disruptions (Apple, 2022). It has standardized its hardware and software systems, enabling it to respond to disruptions and minimize the associated costs quickly and effectively. As a result, Apple maintains its operations during natural disasters and supplier disruptions, reducing the impact on its business (Finucane et al., 2020). Standardization can help make the cost of BCPs more affordable for companies by enabling them to streamline their processes and reduce complexity (Pramudya & Fajar, 2019). Organizations can adopt standardized solutions to ensure that their BCPs are effective and affordable, allowing them to recover quickly during a crisis or disruption while minimizing the associated costs.

Recommendations to Educate Organizations on the Risks of Inadequate BCPs

Recommendation 1: Awareness campaigns

These campaigns can help organizations understand the importance of BCPs and the cost of not having them. The campaigns can target senior management, decision-makers, and employees to ensure that everyone in the organization understands the impact of disruptions and the importance of BCPs. A study by Mavrodieva et al. (2019) found that 57% of SMEs in Indonesia understood the benefits of technical assistance and training on BCPs. Most businesses also expressed readiness to participate in national disaster preparedness campaigns. These statistics highlight the significant need for awareness and training campaigns to enhance preparedness and resilience against disasters in SMEs and large corporations.

To raise awareness about the importance of BCPs, companies can leverage various communication channels and strategies to reach their target audiences. For example, they might create informational videos, webinars, or white papers highlighting the risks of not having a solid BCP and share them through social media, email campaigns, or targeted advertising (Yasin et al., 2020). Effective awareness campaigns can play a critical role in helping companies to understand the risks of operating without adequate BCPs, and in encouraging them to take the necessary steps to protect their businesses and ensure long-term sustainability.

Recommendation 2: Case Studies and Real-World Examples

Case studies and real-world examples can be used to demonstrate the impact of disruptions on organizations that do not have adequate BCPs. These examples can be shared through various mediums, such as webinars, workshops, and training sessions, to help organizations understand their potential risks and the cost of not having BCPs. In 2017, Equifax, one of the largest credit reporting agencies in the United States, experienced a massive cyber-attack that compromised the personal data of approximately

143 million individuals. The breach included sensitive information such as social security numbers, birth dates, and addresses, making it one of history's most damaging data breaches (Gaglione Jr, 2019). The attack had significant consequences for Equifax, including a loss of customer trust, a decline in the company's stock price, and numerous lawsuits and regulatory investigations (Zou et al., 2019). The breach exposed the potential risks of cyber-attacks and the need for companies to have strong cybersecurity measures to protect their data and systems.

Equifax had to implement a robust BCP that included providing free credit monitoring to affected customers, improving their cybersecurity infrastructure, and implementing more robust data protection policies to recover. However, the fallout from the attack highlighted the potential costs of not having a solid BCP, including damage to a company's reputation, loss of revenue, and legal liability (Zou et al., 2019). Case studies such as the Equifax breach can be used to educate companies on the risks of inadequate BCPs in several ways. Firstly, case studies can highlight the real-world consequences of cyber-attacks and data breaches and demonstrate the financial and reputational costs of not having a solid BCP (Gaglione, 2019). By providing concrete examples of how unexpected events have impacted other companies, awareness campaigns can help underscore the importance of BCPs and the need for ongoing preparedness. Secondly, case studies can provide valuable insights into companies' steps to recover from a cyber-attack and mitigate the damage. By analyzing the response strategies and recovery efforts of companies such as Equifax, other organizations can learn from their experiences and identify best practices for responding to similar events in the future (Zou et al., 2019). Case studies can help raise awareness about specific industries or sectors' potential risks and vulnerabilities, highlighting the need for targeted cybersecurity and BCP measures (Wang & Johnson, 2018). For example, the Equifax breach exposed vulnerabilities in the credit reporting industry and prompted many companies in the sector to reevaluate their data protection policies and practices.

Recommendation 3: Compliance Requirements

Regulatory bodies can make it mandatory for organizations to have BCPs. This can encourage organizations to invest in BCPs and ensure that they have adequate measures to minimize the impact of disruptions. For example, the Federal Financial Institutions Examination Council (FFIEC) requires financial institutions to have BCPs. Compliance requirements and bodies can be essential in educating companies on the risks of operating without adequate BCPs. For example, regulatory bodies such as the US Securities and Exchange Commission (SEC) require publicly traded companies to disclose material risks and uncertainties, including those related to business continuity and disaster recovery (Balibek, Storkey, & Yavuz, 2021). By mandating that companies disclose their preparedness measures and risk management strategies, regulatory bodies can help to raise awareness about the importance of BCPs and encourage companies to take steps to mitigate their risks.

Compliance requirements such as the Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA) can also help to educate companies on the importance of BCP (Shuaib et al., 2021). For example, PCI DSS requires companies that process credit card payments to implement strong data security measures, including disaster recovery and business continuity planning (Haldane et al., 2021). Similarly, HIPAA requires healthcare organizations to implement disaster recovery and contingency planning measures to ensure the confidentiality, integrity, and availability of electronically protected health information (ePHI) (Shuaib et al., 2021).

By leveraging compliance requirements and bodies, companies can be held accountable for their preparedness and protection measures and incentivized to invest in BCPs and cybersecurity measures. For

example, companies that fail to comply with regulatory requirements may face fines, legal liability, and reputational damage, which can be a strong motivator for improving their preparedness and protection measures (Balibek, Storkey, & Yavuz, 2021).

Compliance requirements and bodies can help to educate companies on the risks of operating without adequate BCPs by mandating disclosure of preparedness measures and incentivizing investment in risk mitigation strategies (Kollmer et al., 2023). By raising awareness about the importance of BCPs and cybersecurity standards, regulatory bodies and compliance requirements can help to encourage more companies, including Fortune 500 companies, to invest in preparedness and protection measures to safeguard their operations and assets.

Recommendation 4: Financial Incentives

Governments can provide financial incentives to organizations that invest in BCPs. These incentives can include tax breaks, grants, or low-interest loans to help organizations offset the cost of investing in BCPs. According to Mavrodieva et al. (2019), governments greatly provide SMEs incentives during disasters. Financial incentives include grants, conditional cash transfers, tax credits, and subsidies. Non-financial incentives include providing training for risk assessment and providing access to technology and information (Mavrodieva et al., 2019). This can encourage organizations to invest in BCPs and ensure that they have adequate measures to minimize the impact of disruptions. Financial incentives can be used to encourage Fortune 500 companies to invest in information systems for BCP (Mol, Botzen, & Blasch, 2020). For example, insurance companies may offer reduced premiums or better coverage terms to companies demonstrating vital preparedness and protection measures, including robust BCPs and cybersecurity measures.

Financial incentives can also encourage companies to participate in collaborative industry-wide initiatives like information sharing and threat intelligence programs. For example, financial institutions in the US have established the Financial Services Information Sharing and Analysis Center (FS-ISAC), which allows member organizations to share threat intelligence and best practices related to cybersecurity and BCPs (Putra & Aferudin, 2022).

By leveraging financial incentives, companies can be encouraged to invest in information systems for BCP and other risk mitigation measures, which can help to safeguard their operations and assets against unexpected events. However, it is essential to note that financial incentives alone may not be sufficient to ensure that companies take adequate steps to prepare for unforeseen circumstances (Mol, Botzen, & Blasch, 2020). Instead, financial incentives should be used with other educational and awareness-raising initiatives, such as compliance requirements and case studies, to encourage more companies to invest in robust BCPs and cybersecurity measures.

Recommendation 5: Regularly Test and Maintain BCPs

Based on the information provided, Fortune 500 should constantly test and review their business continuity plans (BCPs) and systems to ensure they effectively maintain business operations during disruptions (Fani & Subriadi, 2019). Disturbances, such as the COVID-19 pandemic, can result in unexpected challenges and changes in business operations, making it essential for companies to adapt and update their BCPs and systems to ensure they remain effective (Elsey, 2020; İrkey & Tüfekci, 2021).

Regular testing and maintenance of BCPs and systems can help companies identify gaps and weaknesses in their plans and areas that require improvement or adjustment (Elsey, 2020). By doing so, companies can develop more effective BCPs and systems that better align with their business needs and goals (Fani & Subriadi, 2019). Regular testing and maintenance of BCPs and procedures can help companies ensure

that their minimum metrics and objectives for business continuity are up-to-date and relevant (Elsey, 2020). Regular testing and review of BCPs and systems are critical for companies to maintain business continuity during disruptions. It helps companies identify gaps and weaknesses in their plans and ensure that their business continuity objectives are relevant and current.

Contributions of Study

This explorative study comprehensively analyzes the various information systems the leading Fortune 500 companies deploy to accomplish business continuity in the face of multiple disasters. The selected companies, such as Amazon, Walmart, Toyota, Apple, and GM, leverage innovative systems to achieve business continuity, gain a competitive edge, and maintain optimal operations (Amazon, 2023). Supply chain management, electronic data interchange, customer relationship management, business intelligence, and disaster recovery systems enable these companies to remain competitive post-pandemic.

For instance, Amazon's business intelligence systems offer real-time analytics and insights into the company's operations. BI systems leverage artificial intelligence, machine learning, and big data solutions to provide valuable insights for accurate decision-making, even in disruptions (Gupta & Jiwani, 2021; Goyal et al., 2022). Toyota Production System (TPS) has enabled the company to dominate the automotive industry market share (Carlier, 2022). TPS, a critical component of Toyota's business continuity strategy, has enhanced the company's operational excellence and resilience against disruptions (Haigh, 2022; Shih, 2022). IBM's Resilient Incident Response platform provides real-time monitoring of security incidents and events, enabling an organization to promptly detect and respond to cybersecurity threats and attacks (IBM, 2022). The comprehensive analysis of these systems, including those leveraged in the banking sector and oil and gas industry, provides valuable insights that companies must incorporate in their BCPs. The study also offers evidence-based recommendations for leveraging IS to ensure that the cost of BCPs is affordable and that companies understand the risks of operating without robust BCPs.

Recommendations for Future Research

The case studies leveraged in this study provided valuable and practical insights into how IT-driven companies use information systems to achieve business continuity. Analyzing multiple cases, including the Fortune 500 companies, oil and gas, and banking industries, provided credible insights and diverse findings. However, case studies have limitations, including a perceived lack of rigor, limited generalizability of results, and the possibility of bias (Glette & Wiig, 2022). Though these limitations were addressed by following a structured methodological procedure and using multiple cases and data sources, future research can do better (Yin, 2018). Firstly, future research can leverage mixed-method research to investigate how information systems can reduce the cost of creating and deploying BCPs in IT-driven companies. Future studies can leverage both quantitative and qualitative data collection methods. An analysis of quantitative and qualitative data will provide more insights into this contentious issue (Saunders, Lewis, & Thornhill, 2009).

Secondly, future research should explore how specific information systems are leveraged in particular sectors to achieve business continuity. For example, future studies can investigate how business intelligence systems are leveraged to achieve business continuity in the retail industry. Finally, future research should explore how emerging trends such as artificial intelligence, deep learning, and machine learning can enhance business continuity and resilience to specific disasters such as ransomware attacks and DDoS attacks (Phillips & Landahl, 2020). Consequently, leveraging a hybrid of methodologies and focusing on specific information systems for business continuity will provide more diverse and valuable insights.

References

1. Aasi, P., Hajdari, H., & Yousif, M. (2020). Aligning the information technology leadership with the organizational working environment changes during the pandemic crisis: a case of a large Swedish Medical Institute. *Proceedings ISSN*, *1613*, 0073. https://ceur-ws.org/Vol-3223/paper8.pdf
2. Amazon AWS. (2023). Business continuity planning (BCP). https://aws.amazon.com/local/hongkong/bcp/
3. Apple. (2022). Intro to Apple business manager. *Apple Business Manager User Guide*. https://support.apple.com/en-ke/guide/apple-business-manager/axmd344cdd9d/web#
4. Acciarini, C., Boccardelli, P., & Vitale, M. (2021). Resilient companies in the time of COVID-19 pandemic: a case study approach. *Journal of Entrepreneurship and Public Policy*, *10*(3), 336-351.
5. AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & Security*, *99*, 102030.
6. Aquino, D. H., Wilkinson, S., Raftery, G. M., & Potangaroa, R. (2019). Building back towards storm-resilient housing: Lessons from Fiji's Cyclone Winston experience. *International Journal of Disaster Risk Reduction*, *33*, 355-364.
7. Algarni, S. (2021). Cybersecurity attacks: Analysis of "WannaCry" attacks and proposing methods for reducing or preventing such attacks in the future. In *ICT Systems and Sustainability: Proceedings of ICT4SD 2020, Volume 1* (pp. 763-770). Springer Singapore.
8. Aljuhani, A. (2021). Machine learning approaches for combating distributed denial of service attacks in modern networking environments. *IEEE Access*, *9*, 42236-42264.
9. Angel, D. (2022). Protection of medical information systems against cyber attacks: a graph theoretical approach. *Wireless Personal Communications*, *126*(4), 3455-3464.
10. Armenatzoglou, N., Basu, S., Bhanoori, N., Cai, M., Chainani, N., Chinta, K., ... & Terry, D. (2022, June). Amazon Redshift re-invented. In *Proceedings of the 2022 International Conference on Management of Data* (pp. 2205-2217).
11. Berdermann, J., Kriegel, M., Banyś, D., Heymann, F., Hoque, M. M., Wilken, V., ... & Jakowski, N. (2018). Ionospheric response to the X9. 3 Flare on September 6th, 2017, and its implication for navigation services over Europe. *Space Weather*, *16*(10), 1604-1615.
12. Balibek, M. E., Storkey, I., & Yavuz, H. (2021). *Business continuity planning for government cash and debt management*. International Monetary Fund.
13. Bharadwaj, S. (2019). The engineering behind a successful supply chain management strategy: an insight into Amazon.com. *International Journal of Scientific and Technology Research*, *8*(10), 281-286.

14. Bobel, V. A. D. O., Sigahi, T. F., Rampasso, I. S., Moraes, G. H. S. M. D., Ávila, L. V., Leal Filho, W., & Anholon, R. (2022). Analysis of the level of adoption of business continuity practices by Brazilian industries: an exploratory study using Fuzzy TOPSIS. *Mathematics*, *10*(21), 4041.
15. Brodeur, A., & Yousaf, H. (2022). On the economic consequences of mass shootings. *The Review of Economics and Statistics*, 1-43.
16. Campbell, J. D., & Brown, D. G. (2015). Business continuity and disaster recovery planning for IT professionals. John Wiley & Sons.
17. *Continuity Resource Toolkit*. (2020). FEMA.gov. https://www.fema.gov/emergency-managers/national-preparedness/continuity/toolkit
18. Chang, S. E., Brown, C., Handmer, J., Helgeson, J., Kajitani, Y., Keating, A., ... & Roa-Henriquez, A. (2022). Business recovery from disasters: Lessons from natural hazards and the COVID-19 pandemic. *International Journal of Disaster Risk Reduction*, *80*, 103191.
19. Chakraborty, B., & Chowdhury, Y. (2020). *Introducing disaster recovery with Microsoft Azure*. Apress.
20. Chapple, M., Stewart, M., & Gibson, D. (2018). *Certified Information Systems Security Professional (CISSP): Official Study Guide*. John Wiley & Sons.
21. Corrales-Estrada, A. M., Gómez-Santos, L. L., Bernal-Torres, C. A., & Rodriguez-López, J. E. (2021). Sustainability and resilience organizational capabilities to enhance business continuity management: A literature review. *Sustainability*, *13*(15), 8196.
22. Cao, P. (2021, December). Big data in customer acquisition and retention for ecommerce–taking Walmart as an example. In *2021 3rd International Conference on Economic Management and Cultural Industry (ICEMCI 2021)* (pp. 259-262). Atlantis Press.
23. Carlier, M. (2022). Global automotive market share in 2021 by brand. *Statista*. https://www.statista.com/statistics/316786/global-market-share-of-the-leading-automakers/
24. Centeno, C. (2022). GM's OnStar opens new command center in South America. https://gmauthority.com/blog/2022/07/gms-onstar-opens-new-command-center-in-south-america/
25. Cooper, M. (2013). Walmart takes a collaborative approach to disaster recovery. https://www.pwc.com/gx/en/capital-projects-infrastructure/disaster-resilience/assets/pdf/interview-mark-cooper.pdf
26. Da-Yu, K. A. O., Hsiao, S. C., & Raylin, T. S. O. (2019, February). Analyzing WannaCry ransomware considering the weapons and exploits. In *2019 21st International Conference on Advanced Communication Technology (ICACT)* (pp. 1098-1107). IEEE.
27. Data Foundry. (2019). How much should you spend on business continuity and disaster recovery? https://www.datafoundry.com/blog/much-spend-business-continuity-disaster-recovery
28. Dzulhikam, D., & Rana, M. E. (2022, March). A critical review of cloud computing environment for big data analytics. In *2022 International Conference on Decision Aid Sciences and Applications (DASA)* (pp. 76-81). IEEE.
29. De Preter, S. (2021). Working toward a managed, mature business continuity plan. *ISACA Journal*. https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/working-toward-a-managed-mature-business-continuity-plan#
30. Donovan, A., Suppasri, A., Kuri, M., & Torayashiki, T. (2018). The complex consequences of volcanic warnings: Trust, risk perception and experiences of businesses near Mount Zao following the 2015 unrest period. *International Journal of Disaster Risk Reduction*, *27*, 57-67.

31. Dolezel, D., & McLeod, A. (2019). Cyber-analytics: identifying discriminants of data breaches. *Perspectives in Health Information Management*, *16*(Summer).
32. Extrasio. (2022a). Intelligent BCP Automation. https://www.xtras.io/bcp/
33. Extrasio. (2022b). Leading global IT/ ITSE player improves productivity by 10X. https://www.xtras.io/wp-content/uploads/2016/02/Use%20Case_IT_iBOTS.pdf
34. Extrasio. (2022c). Leading bank achieves intelligent service availability management across its 40 critical applications. https://www.xtras.io/wp-content/uploads/2016/02/Use%20Case_Banking_BCP.pdf
35. Elsey, W. (2020). How and why to create a business continuity plan. *Forbes*. https://www.forbes.com/sites/forbesbusinessdevelopmentcouncil/2020/05/07/how-and-why-to-create-a-business-continuity-plan/?sh=229203654317
36. Esquivel-Vargas, H., Caselli, M., Tews, E., Bucur, D., & Peter, A. (2019). BACRank: ranking building automation and control system components by business continuity impact. In *Computer Safety, Reliability, and Security: 38th International Conference, SAFECOMP 2019, Turku, Finland, September 11–13, 2019, Proceedings 38* (pp. 183-199). Springer International Publishing.
37. Fani, S. V., & Subriadi, A. P. (2019). Business continuity plan: examining of the multi-usable framework. *Procedia Computer Science*, *161*, 275-282.
38. Fakieh, B., & Happonen, A. (2023). Exploring the social trend indications of utilizing e-commerce during and after COVID-19's hit. *Behavioral Sciences*, *13*(1), 5.
39. Federal Reserve Board. (2017). Regulation YY requests. https://www.federalreserve.gov/supervisionreg/regulation-yy-foreign-banking-organization-requests.htm
40. Filipović, D., Krišto, M., & Podrug, N. (2021). Impact of crisis situations on the development of business continuity management in Croatia. *Management Journal of Contemporary Management Issues*, *23*(1), 99–122. https://doi.org/10.30924/mjcmi/2018.23.1.99
41. Finucane, M.L., D'Souza, N., Kates, R.W., Peek, L., Garschagen, M., & Wisner, B. (2020). Short-term solutions to a long-term challenge: Rethinking disaster recovery planning to reduce vulnerabilities and inequities. *International Journal of Disaster Risk Reduction*, 50, 101766.
42. Galbusera, L., Cardarilli, M., & Giannopoulos, G. (2021). The ERNCIP survey on COVID-19: Emergency & Business Continuity for fostering resilience in critical infrastructures. *Safety Science*, *139*, 105161.
43. Ganesha, H., & Aithal, P. (2022). Why is it called a Doctor of Philosophy and why choosing an appropriate research philosophical paradigm is indispensable during ph. d. program in india? *International Journal of Philosophy and Languages (IJPL)*, *1*(1), 42-58.
44. Gaglione Jr, G. S. (2019). The Equifax data breach: an opportunity to improve consumer protection and cybersecurity efforts in America. *Buff. L. Rev.*, *67*, 1133.
45. Gupta, K., & Jiwani, N. (2021). A systematic overview of fundamentals and methods of business intelligence. *International Journal of Sustainable Development in Computing Science*, *3*(3), 31-46.
46. Giunipero, L. C., Denslow, D., & Rynarzewska, A. I. (2022). Small business survival and COVID-19-An exploratory analysis of carriers. *Research in Transportation Economics*, *93*, 101087.
47. Goda, K., Kiyota, T., Pokhrel, R. M., Chiaro, G., Katagiri, T., Sharma, K., & Wilkinson, S. (2015). The 2015 Gorkha Nepal earthquake: insights from earthquake damage survey. *Frontiers in Built Environment*, *1*, 8.

48. Goyal, D., Kumar, N., Piuri, V., Paprzycki, M. (2022). Proceedings of the third international conference on information management and machine intelligence - ICIMMI 2021. Springer. https://doi.org/10.1007/978-981-19-2065-3
49. Glette, M. K., & Wiig, S. (2022). The headaches of case study research: A discussion of emerging challenges and possible ways out of the pain. *The Qualitative Report*, *27*(5), 1377-1392.
50. Golovchenko, Y., Buntain, C., Eady, G., Brown, M. A., & Tucker, J. A. (2020). Cross-platform state propaganda: Russian trolls on Twitter and YouTube during the 2016 US presidential election. *The International Journal of Press/Politics*, *25*(3), 357-389.
51. Gqoboka, H., Anakpo, G., & Mishi, S. (2022). Challenges facing ICT use during covid-19 pandemic: the case of small, medium, and micro enterprises in South Africa. *American Journal of Industrial and Business Management*, *12*(9), 1395-1401. 10.4236/ajibm.2022.129077
52. Green, N., Tappin, D., & Bentley, T. (2020). Working from home before, during and after the Covid-19 pandemic: implications for workers and organisations. *New Zealand Journal of Employment Relations*, *45*(2), 5-16.
53. Green, J., Hanckel, B., Petticrew, M., Paparini, S., & Shaw, S. (2022). Case study research and causal inference. *BMC Medical Research Methodology*, *22*(1), 1-8.
54. Groenendaal, J., & Helsloot, I. (2019). Organizational resilience: shifting from planning-driven business continuity management to anticipated improvisation. *Journal of Business Continuity and Emergency Planning*, *14*(2), 102–109. https://europepmc.org/article/MED/33239142
55. Grondys, K., Ślusarczyk, O., Hussain, H. I., & Androniceanu, A. (2021). Risk assessment of the SME sector operations during the COVID-19 pandemic. *International Journal of Environmental Research and Public Health*, *18*(8), 4183.
56. Haldane, V., De Foo, C., Abdalla, S. M., Jung, A. S., Tan, M., Wu, S., ... & Legido-Quigley, H. (2021). Health systems resilience in managing the COVID-19 pandemic: lessons from 28 countries. *Nature Medicine*, *27*(6), 964-980.
57. Hamdani, K., Mills, C., Silva, J., & Battisto, J. (2018). Puerto Rico small businesses and the 2017 hurricanes. *New York: Federal Reserve Bank of New York*.
58. Hatton, T., & Brown, C. (2021). Building adaptive business continuity plans: Practical tips on how to inject adaptiveness into continuity planning processes. *Journal of business continuity & emergency planning*, *15*(1), 44–52. https://pubmed.ncbi.nlm.nih.gov/34465409/
59. Hatton, T., Vargo, J., & Seville, E. (2023). Business recovery from disaster: creating an enabling environment for surviving and thriving. In *Case Studies in Disaster Recovery* (pp. 3-32). Butterworth-Heinemann.
60. Hawash, B., Mokhtar, U. A., Yusof, Z. M., & Mukred, M. (2022). Enhancing business continuity in the oil and gas industry through electronic records management system usage to improve off-site working: a narrative review. *Journal of Information Science Theory and Practice*, *10*(2), 30-44.
61. Haigh, A. (2022). 2022 Automotive industry trends: doubling down on electric and connected cars. *Brand Finance*. https://brandfinance.com/insights/2022-auto-trends
62. Haseeb, M., Hussain, H. I., Ślusarczyk, B., & Jermsittiparsert, K. (2019). Industry 4.0: A solution towards technology challenges of sustainable business performance. *Social Sciences*, *8*(5), 154.
63. Htun, A. R. K. A. R., Maw, T. T., & Khaing, C. (2019). Lean manufacturing, just in time, and Kanban of Toyota production system (TPS). *International Journal of Scientific Engineering and Technology Research*, *8*(1), 469-474.

64. Henderson, M. G., Bent, R., Chen, Y., Delzanno, G. L., Jeffery, C. A., Jordanova, V. K., ... & Engel, M. (2017, December). Impacts of Extreme Space Weather Events on Power Grid Infrastructure: Physics-Based Modelling of Geomagnetically-Induced Currents (GICs) During Carrington-Class Geomagnetic Storms. In *AGU Fall Meeting Abstracts* (Vol. 2017, pp. SA22A-01).
65. Houston, J. B., Schraedley, M. K., Worley, M. E., Reed, K., & Saidi, J. (2019). Disaster journalism: fostering citizen and community disaster mitigation, preparedness, response, recovery, and resilience across the disaster cycle. *Disasters*, *43*(3), 591-611.
66. Hussain, A., Farooq, M. U., Habib, M. S., Masood, T., & Pruncu, C. I. (2021). COVID-19 challenges: can industry 4.0 technologies help with business continuity? *Sustainability*, *13*(21), 11971.
67. IBM. (2022). An introduction to the resilient incident response platform. https://www.ibm.com/support/pages/introduction-resilient-incident-response-platform
68. ISO. (2022). ISO 22301:2019(en) Security and resilience — Business continuity management systems — Requirements. https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-2:v1:en
69. ISO. (2019). *Security and Resilience: Business Continuity Management Systems-Requirements*. International Organization for Standardization. https://www.iso.org/standard/71916.html
70. ISO. (2022). ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements. Available at: https://www.iso.org/standard/75106.html
71. İrkey, T., & Tüfekci, A. (2021). The importance of business continuity and knowledge management during the pandemic period. *Multidisciplinary Digital Publishing Institute Proceedings*, *74*(1), 18. https://doi.org/10.3390/proceedings2021074018
72. Ivanova, N. (2022). People-centered business continuity: a case for inclusive design. *Design Management Journal*, *17*(1), 30-48.
73. Kaur, A., Kumar, A., & Luthra, S. (2021). Business continuity through customer engagement in sustainable supply chain management: outlining the enablers to manage disruption. *Environmental Science and Pollution Research*, *29*(10), 14999–15017. https://doi.org/10.1007/s11356-021-16683-4
74. Kaur, J. (2016). Customer relationship management: A study of CRM policies of different companies. *Global Journal of Finance and Management*, *8*(2), 153-159.
75. Krell, E. (2006). Business continuity management. NY: American Institute of Certified Public Accountants.
76. Kollmer, T., Durani, K., Peterhänsel, F., Eckhardt, A., & Augustin, N. (2023). Exploring Consumers Risk Mitigation Strategies in E-Commerce: A Qualitative Study of High-Risk Transactions.
77. Kutame, F. N., Ochara, N. M., Kadyamatimba, A., Sotnikov, A., Fiodorov, I., & Telnov, Y. (2021). A case study of cloud-based business continuity model. In *CEUR Workshop Proceedings* (pp. 26-35).
78. Keller, R., Ollig, P., & Fridgen, G. (2019). Decoupling, information technology, and the tradeoff between organizational reliability and organizational agility. In *27th European Conference on Information Systems (ECIS)*.
79. Koonin, L. M. (2020). Novel coronavirus disease (COVID-19) outbreak: Now is the time to refresh pandemic plans. *Journal of Business Continuity & Emergency Planning*, *13*(4), 298-312

80. Kumar, Y. R., Basha, N., KM, K. K., Sharma, B. M., & Kerekovski, K. (2019). *Oracle High Availability, Disaster Recovery, and Cloud Services: Explore RAC, Data Guard, and Cloud Technology*. Apress.
81. Kushma, J. (2022). *Case Studies in Disaster Recovery: A Volume in the Disaster and Emergency Management: Case Studies in Adaptation and Innovation Series*. Butterworth-Heinemann.
82. Kure, H. I., & Islam, S. (2019). Assets focus risk management framework for critical infrastructure cybersecurity risk management. *IET Cyber-Physical Systems: Theory & Applications*, *4*(4), 332-340.
83. Leal, R. (2019). Infographic: ISO 22301:2012 vs. ISO 22301:2019 revision – What has changed? *Advisera*. Available at: https://advisera.com/27001academy/blog/2019/12/02/iso-22301-2019-vs-iso-22301-2012-key-changes-infographic/
84. LeCounte, J. F. (2022). Founder-CEOs: Succession planning for the success, growth, and legacy of family firms. *Journal of Small Business Management*, *60*(3), 616-633.
85. Linvill, D. L., Boatwright, B. C., Grant, W. J., & Warren, P. L. (2019). "THE RUSSIANS ARE HACKING MY BRAIN!" investigating Russia's internet research agency's Twitter tactics during the 2016 United States presidential campaign. *Computers in Human Behavior*, *99*, 292-300.
86. Mao, H., Zhang, T., & Tang, Q. (2021). A research framework for determining how artificial intelligence enables information technology service management for business model resilience. *Sustainability*, *13*(20), 11496.
87. Margherita, A., & Heikkilä, M. (2021). Business continuity in the COVID-19 emergency: A framework of actions undertaken by world-leading companies. *Business Horizons*, *64*(5), 683–695. https://doi.org/10.1016/j.bushor.2021.02.020
88. McCrackan, A. (2004). *A practical guide to business continuity assurance*. Artech House. https://ebookcentral.proquest.com/lib/wilmcoll-ebooks/reader.action?docID=227703&ppg=1
89. Meredith, E. S., Jenkins, S. F., Hayes, J. L., Deligne, N. I., Lallemant, D., Patrick, M., & Neal, C. (2022). Damage assessment for the 2018 lower East Rift Zone lava flows of Kīlauea volcano, Hawai'i. *Bulletin of Volcanology*, *84*(7), 65.
90. Muhaise, H., Ejiri, A. H., Muwanga-Zake, J. W. F., & Kareyo, M. (2020). The research philosophy dilemma for postgraduate student researchers. *International Journal of Research and Scientific Innovation (IJRSI)*|, *VII*, 202-204.
91. Mogdil, S., Gil-Garcia, J.R., Turban, E., Sarker, S., & Chauhan, S. (2021). AI technologies and their impact on supply chain resilience during COVID-19. *Information & Management*, 58(2), 102788.
92. Maiorescu, R. D. (2016). Crisis management at General Motors and Toyota: an analysis of gender-specific communication and media coverage. *Public Relations Review*, *42*(4), 556-563.
93. Metzger, J. (2021). How Walmart is navigating the supply chain to deliver this holiday season. https://corporate.walmart.com/newsroom/2021/10/08/how-walmart-is-navigating-the-supply-chain-to-deliver-this-holiday-season
94. Menn, J. (2020). Exclusive: Apple dropped plan for encrypting backups after FBI complained sources. *Reuters*.
95. Microsoft. (2023). Getting started - system center operations manager on-demand assessment. https://learn.microsoft.com/en-us/services-hub/health/getting-started-scom
96. Mol, J. M., Botzen, W. W., & Blasch, J. E. (2020). Risk reduction in compulsory disaster insurance: Experimental evidence on moral hazard and financial incentives. *Journal of Behavioral and Experimental Economics*, *84*, 101500.

97. Muema, F. S. (2020). *Strategies used by retail business managers to address disruptive changes in technology* (Doctoral dissertation, Walden University).
98. Modgil, S., Gupta, S., Stekelorum, R., & Laguir, I. (2021). AI technologies and their impact on supply chain resilience during COVID-19. *International Journal of Physical Distribution & Logistics Management*, *52*(2), 130-149.
99. Mukherjee, M., Chatterjee, R., Khanna, B. K., Dhillon, P. P. S., Kumar, A., Bajwa, S., ... & Shaw, R. (2020). Ecosystem-centric business continuity planning (eco-centric BCP): A post-COVID-19 new normal. *Progress in Disaster Science*, *7*, 100117.
100. Nawari, N. O., & Ravindran, S. (2019). Blockchain and building information modelling (BIM): Review and applications in post-disaster recovery. *Buildings*, *9*(6), 149.
101. Nair, A. (2022). GM develops continuity plan amid China's COVID-19 outbreak. https://www.reuters.com/business/autos-transportation/gm-develops-continuity-plan-amid-chinas-covid-19-outbreak-2022-04-11/
102. Niemimaa, M., Järveläinen, J., Heikkilä, M., & Heikkilä, J. (2019). Business continuity of business models: Evaluating the resilience of business models for contingencies. *International Journal of Information Management*, 49, 208-216. https://doi.org/10.1016/j.ijinfomgt.2019.04.010
103. Nilsson, F., & Tegström, F. (2020). Evaluation of business continuity management: a case study of disaster recovery during the COVID-19 pandemic. *Lund University*.
104. Osama, A. (2019). *Professional SQL server high availability and disaster recovery*. Packt Publishing.
105. Oracle. (2023). Automate ERP cloud security and internal controls: key use cases for risk management cloud. https://www.oracle.com/a/ocom/docs/applications/erp/oracle-risk-management-key-use-cases.pdf
106. Paul, S. K., Chowdhury, P., Moktadir, M. A., & Lau, K. H. (2021). Supply chain recovery challenges in the wake of the COVID-19 pandemic. *Journal of Business Research*, *136*, 316-329.
107. Pescaroli, G., Turner, S., Gould, T., Alexander, D. E., & Wicks, R. T. (2017). Cascading effects and escalations in wide area power failures: a summary for emergency planners (UCL IRDR and London Resilience Special Report 2017-01). *Institute for Risk and Disaster Reduction, University College London.*
108. Phillips, B. D., & Landahl, M. (2020). *Business Continuity Planning: Increasing Workplace Resilience to Disasters*. Butterworth-Heinemann.
109. Phillips, R., & Tanner, B. (2019). Breaking down silos between business continuity and cyber security. *Journal of Business Continuity & Emergency Planning*, *12*(3), 224-232.
110. Polacco, A., & Backes, K. (2018). The Amazon Go concept: implications, applications, and sustainability. *Journal of Business and Management*, *24*(1), 79-92.
111. Pramudya, G. W., & Fajar, A. N. (2019). Business continuity plan using ISO 22301: 2012 in IT solution company (pt. ABC). *Int. J. Mech. Eng. Technol*, *10*(2), 865-872.
112. Project Pro. (2023). How big data analysis helped increase Walmart's sales turnover? https://www.projectpro.io/article/how-big-data-analysis-helped-increase-walmarts-sales-turnover/109
113. Putra, F. A., & Aferudin, F. (2022). Pengembangan financial service information sharing and analysis center (FS-ISAC) di Indonesia dengan Pendekatan ENISA ISAC in a Box. *Info Kripto*, *16*(2), 79-86.

114. Proudfoot, K. (2022). Inductive/Deductive hybrid thematic analysis in mixed methods research. *Journal of Mixed Methods Research*, 15586898221126816.
115. Qi, Q., Tao, F., Cheng, Y., Cheng, J., & Nee, A. Y. C. (2021). New IT-driven rapid manufacturing for emergency response. *Journal of Manufacturing Systems*, *60*, 928-935.
116. Quebedeaux, L. K. (2013). *Planning for disaster recovery and resilient communities with faith-based and secular nonprofit organizations*. The University of Houston-Clear Lake.
117. Rasiah, R., Kaur, H., & Guptan, V. (2020). Business continuity plan in the higher education industry: University students' perceptions of the effectiveness of academic continuity plans during COVID-19 pandemic. *Applied System Innovation*, *3*(4), 51.
118. Raikes, J., Smith, T. F., Jacobson, C., & Baldwin, C. (2019). Pre-disaster planning and preparedness for floods and droughts: A systematic review. *International Journal of Disaster Risk Reduction*, *38*, 101207.
119. Raina, R. (2022). Moving Crisis to Opportunities: A corporate perspective on the impact of compassionate empathic behaviour on the well-being of employees. *International Journal of Global Business and Competitiveness*, *17*(2), 239-255.
120. Röglinger, M., Plattfaut, R., Borghoff, V., Kerpedzhiev, G., Becker, J., Beverungen, D., & Trkman, P. (2022). Exogenous Shocks and business process management. *Business & Information Systems Engineering*, 1-19. https://doi.org/10.1007/s12599-021-00740-w
121. Rostek, K., Wiśniewski, M., & Skomra, W. (2022). Analysis and evaluation of business continuity measures employed in critical infrastructure during the COVID-19 pandemic. *Sustainability*, *14*(22), 15388.
122. Rosenberg, J., & Tombini, A. (2022). Business continuity planning at central banks during and after the pandemic - Consultative Group on Risk Management. *Bank of International Settlements.*
123. Russo, N., São Mamede, H., Reis, L., & Silveira, C. (2022). FAMMOCN–Demonstration and evaluation of a framework for the multidisciplinary assessment of organisational maturity on business continuity. *Heliyon*, *8*(9), e10566.
124. Rundle, J. B., Luginbuhl, M., Giguere, A., & Turcotte, D. L. (2019). Natural time, nowcasting and the physics of earthquakes: Estimation of seismic risk to global megacities. *Earthquakes and Multi-hazards Around the Pacific Rim, Vol. II*, 123-136.
125. Said, N. B., & Chiang, V. C. (2020). The knowledge, skill competencies, and psychological preparedness of nurses for disasters: a systematic review. *International Emergency Nursing*, *48*, 100806.
126. Sakurai, M., & Murayama, Y. (2019). Information technologies and disaster management–benefits and issues. *Progress in Disaster Science*, *2*, 100012. https://doi.org/10.1016/j.pdisas.2019.100012
127. Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods for business students*. Pearson education.
128. Schmidt, D. H., Garland, K., & Quebedeaux, L. K. (2023). Resilient recovery strategies: lessons from the local nonprofit sector following Hurricane Ike. In *Case Studies in Disaster Recovery* (pp. 33-51). Butterworth-Heinemann.
129. Smith, S. M., & Albaum, G. S. (2012). Basic marketing research: volume 1. handbook for research professionals. *Provo: Qualtrics Labs Inc.*
130. Srivastava, R. (2020). Role of information systems in business continuity plans in the context of COVID-19. *International Journal of Emerging Technologies and Applied Sciences*, 1(2), pp.25-29.

131. Soufi, R. H., Torabi, S. A., & Sahebjamnia, N. (2019). Developing a novel quantitative framework for business continuity planning. *International Journal of Production Research*, *57*(3), 779–800. https://doi-org.mylibrary.wilmu.edu/10.1080/00207543.2018.1483586
132. Salhab, N., Rahim, R., & Langar, R. (2020). Optimization of virtualization cost, processing power, and network load of 5G software-defined data centers. *IEEE Transactions on Network and Service Management*, *17*(3), 1542-1553.
133. Sharma, P., & Dash, B. (2023). Smart SCM using AI and Microsoft 365. *International Journal of Advanced Research in Computer and Communication Engineering*, *12*(1).
134. Shih, W. (2022). What really makes Toyota's production system resilient? *Harvard Business Review*. https://hbr.org/2022/11/what-really-makes-toyotas-production-system-resilient
135. Shi, C., & Veres, S. M. (2021). Concepts of self-maintaining robots and their design. *arXiv preprint arXiv:2110.05882*.
136. Siderska, J. (2021). The adoption of robotic process automation technology to ensure business processes during the COVID-19 pandemic. *Sustainability*, *13*(14), 8020.
137. Shuaib, M., Alam, S., Alam, M. S., & Nasir, M. S. (2021). Compliance with HIPAA and GDPR in the blockchain-based electronic health record. *Materials Today: Proceedings*.
138. Supriadi, L. S. R., & Pheng, L. S. (2018). *Business continuity management in construction*. Springer Singapore.
139. Tammineedi, R. L. (2010). Business continuity management: a standards-based approach. *Information Security Journal: A Global Perspective*, *19*(1), 36–50. https://doi-org.mylibrary.wilmu.edu/10.1080/19393550903551843
140. Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT privacy and security: challenges and solutions. *Applied Sciences*, *10*(12), 4102.
141. Tyagi, K., Yadav, S. K., & Singh, M. (2021, August). Cloud data security and various security algorithms. In *Journal of Physics: Conference Series* (Vol. 1998, No. 1, p. 012023). IOP Publishing.
142. Thakur, B.R., Kaur, N. and Chahal, G. (2020). Role of information systems in business continuity planning. *International Journal of Scientific Research and Management*, 8(6).
143. Varandani, S. (2016). Cyclone Winston: Fiji's estimated cost of damages exceeds $470M, 10% of the island nation's total GDP. *International Business Times*. Available at: https://www.ibtimes.com/cyclone-winston-fijis-estimated-cost-damages-exceeds-470m-10-island-nationstotal-gdp-2332151.
144. Vogel, G. (2022). Validating business continuity programs in the new normal. *Journal of Business Continuity & Emergency Planning*, *15*(4), 319–329.
145. Viktor, A. (2023). Walmart CRM strategy: a decade-long secret you never knew. https://crmside.com/walmart-crm-strategy/
146. Verlin, K. (2021). Toyota ranks no. 9 in 2021 fortune global 500 list. *The News Wheel*. https://thenewswheel.com/toyota-ranks-no9-2021-fortune-global-500/
147. Wallace, M., & Webber, L. (2017). *The disaster recovery handbook: A step-by-step plan to ensure business continuity and protect vital operations, facilities, and assets*. Amacom.
148. Walmart. (2022). EDI System. https://walmartsupplychain.weebly.com/edi-system.html
149. Wayland, M. (2021). Toyota tops GM sales in the US, expected to be America's bestselling automaker. *CNBC*. https://www.cnbc.com/2021/07/01/toyota-tops-gm-sales-expected-to-be-americas-best-selling-automaker.html

150. Wang, P., & Johnson, C. (2018). Cybersecurity incident handling: a case study of the Equifax data breach. *Issues in Information Systems*, *19*(3).
151. Wong, W., & Shi, J. (2015). *Business continuity management system: a complete guide to implementing iso 22301*. Kogan Page Publishers.
152. World Bank. (2020). Resilient industries in Japan: lessons learned in Japan on enhancing competitive industries in the face of disasters caused by natural hazards. *World Bank, Washington, D.C.*
153. Yale University. (2019). *Business Continuity for Clinical Practices | Emergency Management*. https://emergency.yale.edu/planning/business-continuity-planning/clinical-practice
154. Yin, R. K. (2018). *Case study research and applications: design and methods*. 6th ed. Thousand Oaks, California: Sage Publications Inc.
155. Yasin, M., Liébana-Cabanillas, F., Porcu, L., & Kayed, R. N. (2020). The role of customer online brand experience in customers' intention to forward online company-generated content: The case of the Islamic online banking sector in Palestine. *Journal of Retailing and Consumer Services*, *52*, 101902.
156. Zawada, B., & Perry, M. (2020). Framing business continuity to achieve lasting focus. *Journal of Business Continuity & Emergency Planning*, *13*(3), 211–219. http://mylibrary.wilmu.edu/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=bsu&AN=142184605&site=ehost-live
157. Zeng, Z., & Zio, E. (2017). An integrated modelling framework for quantitative business continuity assessment. *Process Safety & Environmental Protection: Transactions of the Institution of Chemical Engineers Part B*, *106*(Part B), 76–88.
158. Zou, Y., Mhaidli, A. H., McCall, A., & Schaub, F. (2018, August). " I've got nothing to lose": consumers' risk perceptions and protective actions after the Equifax data breach. In *SOUPS@ USENIX Security Symposium* (pp. 197-216).