Ensuring resilience: Integrating IT disaster recovery planning and business continuity for sustainable information technology operations

Derick Musundi Kesa *

Jaramogi Oginga Odinga University of Science & Technology, Kenya.

World Journal of Advanced Research and Reviews, 2023, 18(03), 970–992

Publication history: Received on 07 May 2023; revised on 16 June 2023; accepted on 19 June 2023

Article DOI: https://doi.org/10.30574/wjarr.2023.18.3.1166

Abstract

Information Technology (IT) Disaster Recovery Planning (IT DRP) and Business Continuity (BC) are essential components of an organization's overall resilience strategy. IT DRP focuses on the recovery and restoration of IT systems, infrastructure, and services in the event of a disruptive incident or disaster, aiming to minimize downtime and data loss. BC, on the other hand, encompasses a broader perspective, addressing the organization's ability to maintain essential operations and deliver critical services during and after a disruption. This paper provides an overview of IT DRP and BC, highlighting their importance, challenges, and strategies. It also identifies the research gaps and future research scope in these areas. The findings indicate that both IT DRP and BC face challenges in their effective implementation. These challenges include the evolving nature of technology, increasing complexity of IT systems, budget constraints, organizational resistance to change, and the need for skilled personnel. Overcoming these challenges requires a comprehensive understanding of the organization's IT infrastructure, risk assessment, and the development of robust recovery strategies and plans. It is also noted that despite considerable research on IT DRP and BC, there are several research gaps that deserve attention. These include the development of advanced technologies and tools for more efficient recovery and continuity, the integration of IT DRP and BC with overall organizational risk management, the impact of emerging technologies such as cloud computing and virtualization on recovery strategies, and the evaluation of the effectiveness and cost-efficiency of different IT DRP and BC strategies.

Keywords: Information Technology; Business Continuity; Disaster Recovery; IT DRP; BC

1. Introduction

IT disaster recovery planning is the process of developing strategies, policies, and procedures to recover and restore IT systems, infrastructure, and services after a disruptive incident or disaster [1]-[4]. It involves a systematic approach to ensure the continuity of critical IT operations, minimize downtime, and protect data integrity [5], [6]. The primary goal of IT DRP is to enable the organization to recover IT capabilities and resume normal business operations as quickly and efficiently as possible. On the other hand, IT business continuity refers to the ability of an organization to continue its essential IT operations and deliver critical services during and after a disruptive incident or disaster [7]. It involves having strategies, plans, and measures in place to ensure that IT systems, infrastructure, and services can operate without significant interruption, even in the face of adverse events. According to [8], IT business continuity focuses on maintaining the availability, functionality, and resilience of IT assets and processes to support the organization's overall business continuity objectives. The following sections discuss these concepts in some greater details.

*Corresponding author: Derick Musundi Kesa

2. Disaster Recovery Planning

IT Disaster Recovery Planning encompasses the systematic process that organizations undertake to develop strategies, policies, and procedures for recovering and restoring their IT infrastructure, systems, and services in the event of a disruptive incident or disaster [9], [10]. It focuses specifically on the recovery and restoration of IT capabilities to minimize downtime, data loss, and the impact on business operations. Figure 1 shows a typical data recovery planning. According to [11], the purpose of IT disaster recovery planning is to ensure that an organization's critical IT systems and services can be recovered and restored within predefined timeframes and with minimal disruption to business operations. It involves a series of activities for the identification of potential risks and vulnerabilities [12], the development of a recovery strategy, and the establishment of detailed procedures and protocols for executing the recovery process. According to [13], the key components of IT disaster recovery planning include risk assessment and business impact analysis, recovery objectives, recovery strategies, backup and data recovery, recovery procedures, communication and notification, as well as testing and maintenance. Researchers in [14] and [15] explain that risk assessment and business impact analysis involves identifying potential risks and threats to the organization's IT infrastructure, systems, and services. This involves assessing the potential impact of these risks on the organization's operations, revenue, customer satisfaction, and regulatory compliance.

Figure 1 Data recovery planning

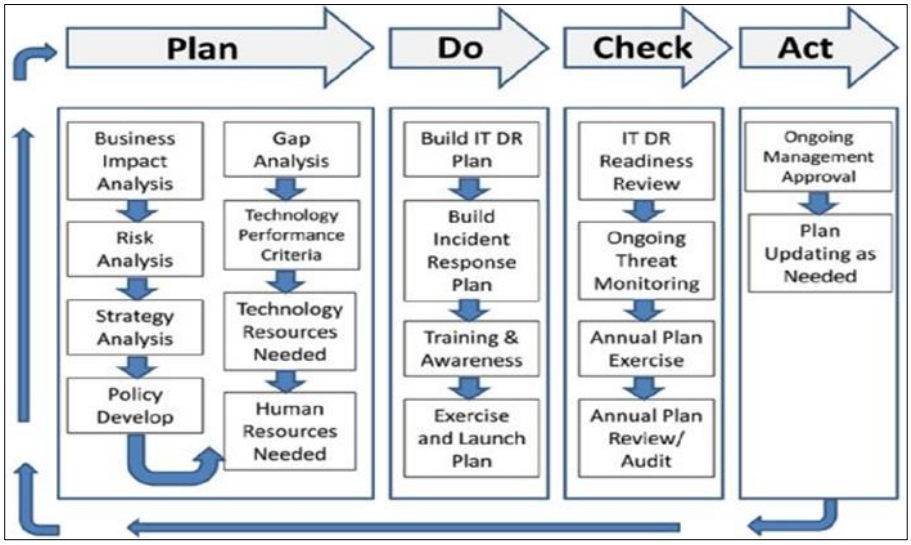

Figure 2 Activities in IT disaster recovery

Establishing recovery objectives such as Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) is important [16]. This is because these objectives define the maximum acceptable downtime and data loss tolerances for different IT systems and services. These objectives help determine the priorities and resources [17] required for recovery efforts. On the other hand, recovery strategies involve the development of approaches based on the identified risks and recovery objectives [18], [19]. This includes determining the most suitable methods and approaches for recovering IT systems and services, such as restoring from backups, activating redundant systems, or utilizing alternative infrastructure. Regarding backup and data recovery, the process entails the implementation of data backup and recovery mechanisms to protect critical data and ensure its availability for restoration [21], [22]. This involves regular and reliable backup processes, offsite storage of backups, and the testing of data recovery procedures to validate their effectiveness [23]. Figure 2 details the activities involved in IT disaster recovery.

According to [24], recovery procedures deal with the definition of detailed step-by-step procedures for executing the recovery process. These procedures outline the specific actions to be taken during different stages of the recovery, including system startup, data restoration, network reconfiguration, and application recovery. On the other hand, communication and notification encompasses the establishment of communication channels and protocols to ensure timely and effective communication during the recovery process [25]. This includes notifying key stakeholders, coordinating with relevant teams and departments, and providing updates on the progress of the recovery efforts. As explained in [26] and [27], testing and maintenance deals with regular testing of the IT disaster recovery plan through simulations and exercises to validate its effectiveness and identify any gaps or areas for improvement. Additionally, it involves conducting routine maintenance and updates to ensure that the plan remains current and aligned with the organization's evolving IT infrastructure and systems.

2.1. Steps in IT disaster recovery planning

IT disaster recovery planning is a crucial component of an organization's overall business continuity strategy [28], [29]. By implementing a well-designed and comprehensive IT DRP, organizations can minimize the impact of disruptive incidents, protect critical data [30] and systems, and ensure the timely recovery and restoration of their IT capabilities. According to [31], IT disaster recovery planning encompasses steps such as risk assessment, business impact analysis (bia), recovery objectives, recovery strategies, plan development, data backup and recovery, testing and exercising, as well as training and awareness. Figure 3 shows a typical disaster recovery plan.

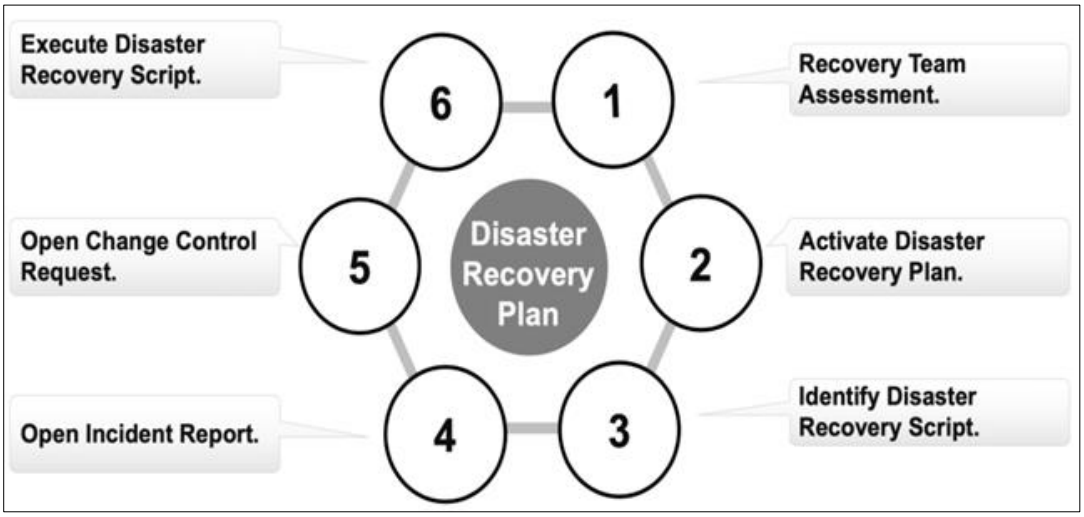

Figure 3 Disaster recovery plan

Table 1 describes these disaster recovery planning steps in details

In a nutshell, IT disaster recovery planning is an ongoing process that requires regular review, updates, and maintenance to ensure its effectiveness in the face of evolving risks, technologies [61], and business requirements. By following a structured approach and implementing an IT disaster recovery plan, organizations can mitigate the impact of disruptions, protect critical IT systems and data, and minimize the downtime associated with a disaster.

Table 1 Steps in IT disaster recovery planning

Step	Activities
Risk assessment	Deals with identifying potential risks and vulnerabilities that could impact IT systems and services [32], [33]. This involves analyzing threats such as natural disasters, cyber-attacks, hardware failures, power outages, and human errors. The risk assessment helps determine the likelihood and potential impact of these risks on IT operations.
Business Impact Analysis (BIA)	Involves assessing the criticality of IT systems and services to the organization's overall business operations. This involves identifying the dependencies and interconnections between IT and other business functions [35], [36]. The BIA helps prioritize IT resources and recovery efforts based on their impact on the organization's productivity, revenue generation, customer satisfaction, and regulatory compliance.
Recovery objectives	Concerned with defining recovery objectives, such as Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). RTO specifies the maximum acceptable downtime for each IT system or service, while RPO defines the acceptable amount of data loss [36]. These objectives guide the development of recovery strategies and the allocation of resources [37] for recovery efforts.
Recovery strategies	Involves developing strategies to restore IT systems and services [38]-[41]. This involves determining the most appropriate recovery methods, such as data restoration from backups, failover to redundant systems, rebuilding infrastructure, or utilizing alternative resources [42]. The selection of recovery strategies depends on factors like the criticality of the system [43], cost considerations, and technical feasibility.
Plan Development	Deals with creation of a comprehensive IT disaster recovery plan that outlines the steps and procedures for executing the recovery process [44]-[48]. The plan includes roles and responsibilities, communication protocols, recovery procedures, and a timeline for each recovery activity. It also addresses resource requirements [49], equipment, software, and data needed for the recovery process.
Data backup and recovery	Deals with establishing mechanisms for regular data backups and secure storage [50]-[54]. This involves defining backup schedules, selecting appropriate backup technologies, and implementing procedures for data recovery. It ensures that critical data can be restored to a known state in the event of data loss or corruption [55].
Testing and exercising	Regularly testing the IT disaster recovery plan through simulations and exercises to validate its effectiveness [56]-[58]. Testing helps identify any weaknesses, refine procedures, and train personnel to ensure a coordinated response during a real incident. It also includes reviewing and updating the plan based on the results of testing and exercises.
Training and awareness	Providing training and awareness programs to IT staff and stakeholders to ensure they understand their roles and responsibilities in executing the IT disaster recovery plan [59], [60]. This includes educating employees on incident response procedures, data protection practices, and the importance of maintaining IT resilience.

2.2. IT disaster recovery planning strategies

IT Disaster Recovery Planning strategies are the specific approaches and techniques employed to recover and restore IT systems, infrastructure, and services in the event of a disruptive incident or disaster [62], [63]. These strategies are designed to minimize downtime, data loss, and the impact on business operations. The common IT DRP strategies include backup and restore, replication and failover, virtualization, cloud-based recovery, mobile recovery, mutual aid agreements, vendor recovery services, data center recovery, testing and maintenance. These strategies are described in detail in Table 2 below.

Table 2 IT disaster recovery planning strategies

Strategy	Activities
Backup and restore	Involves creating regular backups of critical data and systems and restoring them to a pre-disaster state [64]-[66]. It includes implementing backup mechanisms, defining backup schedules, and establishing reliable and secure storage for backups.
Replication and failover	Encompasses creating and maintaining real-time or near-real-time copies of critical data and systems [67] in separate locations. Failover is the process of automatically switching to the replicated system when the primary system fails. This strategy ensures continuous availability and minimizes downtime.
Virtualization	Virtualization allows for the creation of virtual instances of servers, systems, or applications [68]-[71]. This strategy enables rapid recovery by quickly provisioning virtual environments, minimizing hardware dependencies, and facilitating flexible resource allocation.
Cloud-based recovery	Leveraging cloud services for disaster recovery purposes provides scalable and flexible resources that can be quickly deployed in case of a disruption [72], [73]. Cloud-based recovery allows organizations to recover critical systems [74] and data remotely, reducing reliance on physical infrastructure.
Mobile Recovery	Mobile recovery strategies involve the use of mobile devices, portable equipment, or temporary facilities to restore critical IT services [75]. This strategy is useful when the primary location is inaccessible or requires immediate evacuation.
Mutual aid agreements	Mutual aid agreements involve partnerships with other organizations to share resources and support during a disaster [76], [77]. These agreements can include shared data centers, backup sites, or reciprocal arrangements for supporting each other's IT operations during disruptions.
Vendor recovery services	Encompasses engaging with specialized vendors or service providers who offer dedicated recovery services and facilities [78]-[80]. These vendors provide ready-to-use recovery infrastructure [81] and expertise to assist in the recovery process.
Data center recovery	Establishing alternative data center facilities or co-location services to ensure the continuity of IT operations in case of a primary data center failure. This strategy involves replicating critical systems and data in the alternate data center and implementing procedures for failover and recovery [82]-[84].
Testing and maintenance	Regularly testing the IT DRP strategies through simulated exercises and drills to validate their effectiveness [85]. Testing helps identify gaps, refine procedures, and train personnel to ensure a coordinated and efficient response during a real incident. Additionally, routine maintenance and updates should be conducted to keep the plan current and aligned with the evolving IT environment.

The selection and implementation of specific IT DRP strategies depend on various factors such as the organization's IT infrastructure, budget, recovery objectives, and criticality of systems and services. A well-designed combination of these strategies ensures that organizations can effectively recover their IT operations, minimize downtime, and restore critical systems and data in a timely manner.

3. Business continuity

IT business continuity refers to the planning and implementation of strategies and measures to ensure the continuous operation of IT systems and services in the event of a disruptive incident or disaster [86]. As shown in Figure 4, it involves identifying potential risks and vulnerabilities [87] that could impact IT operations, developing a comprehensive plan to mitigate those risks, and establishing procedures to recover IT systems and services quickly and efficiently.

According to [88], the goal of IT business continuity is to minimize downtime, data loss, and service disruptions, enabling organizations to maintain critical IT functions and support their overall business operations. It involves the integration of IT systems, processes, and resources with broader business continuity strategies to ensure that IT

operations align with the organization's overall goals and objectives. The sub-sections below describe business continuity in detail.

Figure 4 Processes in business continuity

3.1. Key components of IT business continuity

The most important ingredients of the business continuity include risk assessment, business impact analysis, business continuity planning, backup and recovery, incident response and management, testing and exercising, training and awareness [89], [90]. As explained in [91] and [92], risk assessment deals with identifying and assessing potential risks and threats to IT systems and services, such as natural disasters, cyber-attacks [93], hardware failures, or human errors. This involves understanding the potential impact of these risks on the organization's IT infrastructure and operations. On the other hand, business impact analysis deals with evaluating the criticality of IT systems and services to the organization's overall business operations [94], [95]. This helps prioritize IT resources and recovery efforts based on their impact on the organization's productivity, revenue generation, customer satisfaction, and regulatory compliance. According to [96], business continuity planning requires the development of a comprehensive plan that outlines the steps and procedures to be followed during and after a disruptive incident. This includes defining roles and responsibilities, establishing communication channels, outlining recovery strategies, and documenting the necessary procedures and guidelines to ensure the continuity of IT operations. The specific activities are depicted in Figure 5.

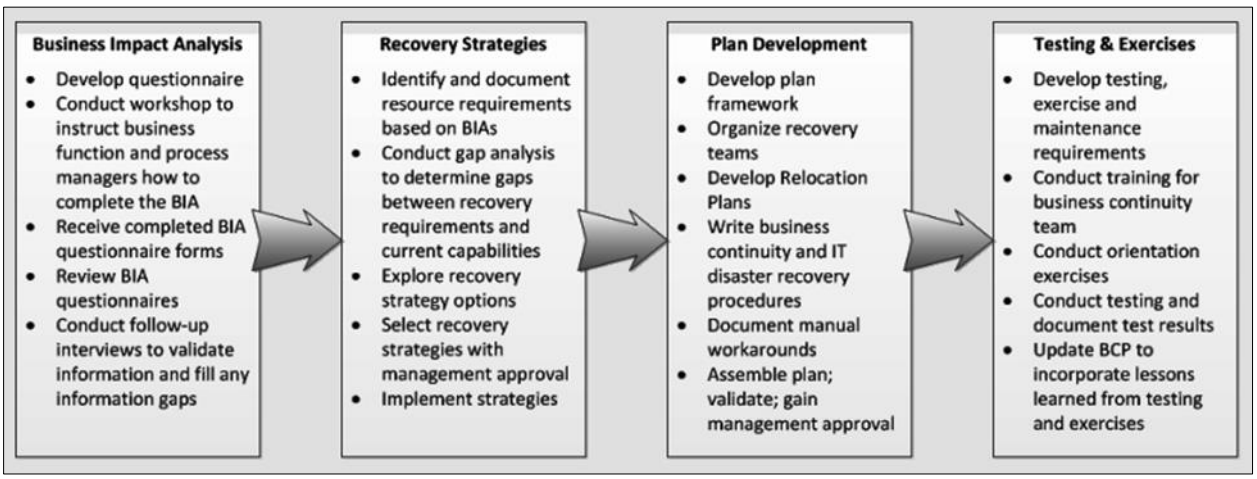

Figure 5 Business continuity plan

Backup and recovery involves the implementation of strategies for regular data backup and establishing mechanisms for efficient data recovery. This involves determining backup schedules, selecting appropriate backup technologies, and testing the recovery procedures to ensure the integrity and availability of critical data and systems [97]-[99]. On the other hand, Incident response and management deals with establishing protocols and procedures to respond to and

manage incidents effectively. This includes early detection and notification, incident containment, investigation, and the implementation of corrective actions to minimize the impact on IT operations and prevent further disruptions. Figure 6 presents the business continuity planning lifecycle.

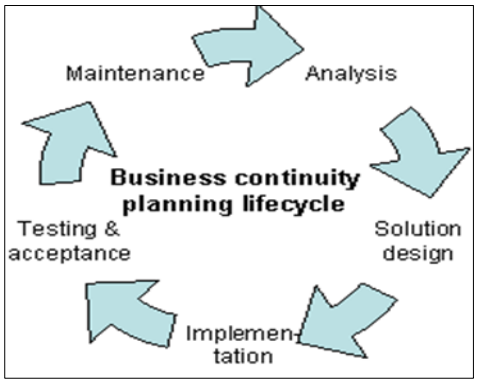

Figure 6 Business continuity planning lifecycle

According to [100], testing and exercising is concerned with regular testing the effectiveness of the IT business continuity plan through simulations, tabletop exercises, or full-scale drills. This helps identify gaps, validate procedures, and train personnel to ensure a coordinated and efficient response during a real incident [101], [102]. On its part, training and awareness is the provision of training and awareness programs to IT staff and stakeholders to ensure they understand their roles and responsibilities in implementing the IT business continuity plan [103], [104]. This includes educating employees on incident response procedures, data protection practices, and the importance of maintaining IT resilience.

In short, IT business continuity is a critical aspect of overall business continuity planning, as it ensures the uninterrupted operation of IT systems and services that are essential for supporting business functions, maintaining customer trust, and meeting regulatory requirements. By effectively implementing IT business continuity strategies, organizations can minimize downtime, recover quickly from disruptions, and ensure the availability and integrity [105] of their IT infrastructure and data.

3.2. IT business continuity important aspects

The most important aspects in IT business continuity include availability of it systems and services, data protection and recovery, infrastructure resilience, incident response and management, business continuity integration, vendor and supplier management, testing and exercises, continuous improvement. The particular details of these concepts are discussed in Table 3 below.

Table 3IT business continuity important aspects

Aspect	Discussion
Availability of IT systems and services	Concerned with ensuring that key IT systems and services required for business operations are available and accessible to users [106]-[108]. This involves implementing redundant systems, failover mechanisms, and load balancing to minimize downtime and ensure continuous service delivery.
Data protection and recovery	Deals with the implementation of measures to protect critical data and enabling its recovery in case of data loss or corruption [109], [110]. This includes regular backups, offsite storage, data replication, and robust recovery procedures to minimize the impact of data-related incidents.
Infrastructure resilience	Involves building resilient IT infrastructure that can withstand disruptions and quickly recover from failures [111]. This involves designing systems with built-in redundancy, fault tolerance, and scalability [112], as well as implementing proactive maintenance and monitoring practices to detect and address issues before they cause significant disruptions.

Incident response and management	Deals with establishment of incident response plans and protocols to effectively manage and mitigate the impact of IT incidents or disruptions. This includes defining roles and responsibilities, establishing communication channels, and implementing incident response procedures to contain and address incidents promptly [113]-[116].
Business continuity integration	Is the alignment of IT business continuity plans with the overall business continuity strategy of the organization [117]. This involves understanding the criticality of IT systems and services to the organization's operations, coordinating with business units to define recovery priorities, and ensuring that IT plans support the overall organizational goals.
Vendor and supplier management	Is the assessment of the business continuity capabilities of third-party vendors and suppliers to ensure that they can provide uninterrupted services [118], [119]. This includes establishing service level agreements (SLAs) that define the expected level of service during disruptions and conducting regular audits or assessments to ensure compliance.
Testing and exercises	Is the conduction of regular testing and exercises to validate the effectiveness of IT business continuity plans and uncover potential weaknesses or gaps [120]. This includes tabletop exercises, simulations, or full-scale drills to evaluate response capabilities, train personnel, and identify areas for improvement.
Continuous improvement	Deals with continuous monitoring and evaluating the effectiveness of IT business continuity strategies, processes, and plans [121]. This involves conducting post-incident reviews, gathering feedback, and incorporating lessons learned into future planning and improvements.

By implementing IT business continuity measures, organizations can minimize the impact of disruptive incidents, maintain the availability of critical IT services, protect data integrity, and support the overall resilience and continuity of their business operations.

3.3. IT business continuity strategies

IT business continuity strategies are the specific approaches and techniques employed to ensure the continuity of IT systems and services during and after a disruptive incident or disaster [122]-[124]. These strategies are designed to minimize the impact of disruptions and enable organizations to recover and resume critical IT operations effectively. Some common IT business continuity strategies include redundancy and failover, data backup and recovery, virtualization and cloud services, disaster recovery sites, incident response and management, business continuity testing, cyber-security measures [125], supplier and vendor management, staff training and awareness. Figure 7 describes some detailed activities executed in these strategies.

Figure 7 Activities in IT business continuity

According to [126], redundancy and failover is concerned with the implementation of redundancy and failover mechanisms to ensure the availability of critical IT systems and services. This involves setting up duplicate hardware, networks, and infrastructure components to automatically take over in the event of a failure, minimizing downtime and ensuring uninterrupted service. On the other hand, data backup and recovery requires the establishment of robust data backup and recovery procedures to protect critical data and enable its restoration in case of data loss or corruption [127]. This includes regular backups of important data, offsite storage, and testing the recovery process to ensure data integrity and availability. Researchers in [128] discuss that virtualization and cloud services deals with the leveraging of virtualization technologies and cloud services to enhance IT resilience. Virtualization allows for the creation of virtual instances of servers and systems, enabling quick recovery and migration in the event of a hardware failure [129]. Cloud services provide scalable and remote infrastructure that can be utilized as an alternative during disruptions [130], [131].

Disaster recovery sites require the setting up of dedicated offsite locations or disaster recovery sites that can house backup systems and infrastructure. These sites serve as alternative operating centers in case the primary site becomes unavailable, ensuring continuity of IT operations [132]. However, incident response and management calls for the establishment of incident response plans and protocols to effectively manage and mitigate the impact of disruptive incidents. This involves defining roles and responsibilities, establishing communication channels, and implementing incident response procedures to contain and address incidents promptly [133], [134]. On the other hand, business continuity testing calls for regular testing of the effectiveness of IT business continuity plans through simulations and exercises. This helps identify weaknesses, validate recovery procedures, and train personnel to ensure a coordinated and efficient response during a real incident [135], [136]. In addition, it is important to implement robust cyber-security measures to protect IT systems and data from cyber threats [137]. This includes using firewalls, intrusion detection and prevention systems, encryption, and access controls to safeguard critical IT infrastructure and prevent unauthorized access or data breaches.

According to [138], supplier and vendor management ensures that third-party suppliers and vendors have robust business continuity plans in place to minimize disruptions to critical services. This involves assessing their preparedness, establishing service level agreements (SLAs), and regularly monitoring their compliance with business continuity requirements. On the other hand, staff training and awareness requires the provision of training and awareness programs to IT staff and employees on the IT business continuity plan [139]. This includes educating them about incident response procedures, data protection practices, and their roles and responsibilities in ensuring the continuity of IT operations.

It is evident that the selection and implementation of specific IT business continuity strategies depend on many factors such as the organization's IT infrastructure, budget, risk appetite, and criticality of IT systems and services. A comprehensive and well-designed combination of these strategies ensures that organizations can effectively respond to disruptions, minimize downtime, and maintain the continuity of IT operations.

4. Challenges of effective Disaster Recovery Planning

Effective IT disaster recovery planning faces several challenges that organizations need to overcome to ensure the continuity of their IT operations. Some of the key challenges are discussed in Table 4 below:

Table 4 Challenges of effective Disaster Recovery Planning

Challenge	Discussion
Complexity of IT infrastructure	Organizations often have complex and interconnected IT infrastructures, consisting of various systems, applications, networks, and data centers [140], [141]. Mapping and understanding the dependencies and interconnections among these components can be challenging, making it difficult to develop a comprehensive and effective disaster recovery plan.
Rapidly evolving technology	The technology landscape is continuously evolving, with new systems, platforms, and software being introduced regularly. Keeping up with these advancements and ensuring that the disaster recovery plan remains up to date and aligned with the changing technology landscape is a significant challenge[142].

Data volume and complexity	Organizations generate and store massive amounts of data, and ensuring its timely backup, replication, and recovery can be challenging [143]. Handling the complexity of diverse data sources, data formats, and data storage systems [144] can make data recovery processes complex and time-consuming.
Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)	Determining appropriate RTOs and RPOs is crucial in disaster recovery planning. Balancing the need for quick recovery with the cost and feasibility of achieving aggressive RTOs and RPOs can be challenging, especially for organizations with limited resources [145], [146].
Resource constraints	Developing and implementing an effective IT disaster recovery plan requires dedicated resources, including financial, technological, and human resources [147]. Limited budgets, resource constraints, and competing priorities can hinder organizations from investing adequately in disaster recovery planning and preparedness activities.
Vendor and supplier dependencies	Organizations often rely on third-party vendors and suppliers for critical IT services, such as cloud hosting or software providers. Managing the risks associated with these dependencies, ensuring their disaster recovery preparedness, and establishing effective communication and coordination mechanisms can be challenging [148], [149].
Testing and exercising	Regular testing and exercising of the IT disaster recovery plan are essential to validate procedures, identify gaps, and enhance response capabilities. However, organizations often face challenges in conducting comprehensive testing due to operational limitations, resource constraints [150], or the fear of disrupting ongoing operations.
Staff awareness and training	Staff awareness and training are crucial for effective disaster recovery planning and execution [151]. Ensuring that IT staff are well-versed in the disaster recovery plan, trained in their roles and responsibilities, and have the necessary technical skills can be challenging, particularly in organizations with a high turnover rate or limited training resources.
Compliance and regulatory requirements	Organizations must comply with various regulatory and compliance requirements related to data protection, privacy, and industry-specific regulations [152]. Incorporating these requirements into the disaster recovery plan and ensuring compliance during the recovery process can be challenging, especially in regulated industries with stringent compliance obligations.

Overcoming these challenges requires a proactive and comprehensive approach. Organizations should allocate sufficient resources, stay updated with technology advancements, conduct regular testing and training, establish effective communication channels, and ensure alignment with regulatory requirements to ensure the effectiveness of their IT disaster recovery planning efforts. Engaging external expertise and leveraging industry best practices can also help organizations address challenges and enhance the effectiveness of their IT disaster recovery planning.

5. Challenges of business continuity planning

IT business continuity planning faces several challenges that organizations need to address effectively. Some of the key challenges are complexity of IT infrastructure, rapidly evolving technology landscape, resource constraints, dependency on third-party service providers, data protection and privacy, testing and exercising, human error and training, changing regulatory and compliance landscape, communication and coordination, as discussed in Table 5 below:

Addressing these challenges requires a proactive and comprehensive approach. Organizations should allocate sufficient resources, stay updated with the evolving technology and regulatory landscape, conduct regular testing and training, establish effective communication channels, and engage stakeholders across the organization to ensure the success of IT business continuity planning efforts.

Table 5 Challenges of business continuity planning

Challenge	Description
Complexity of IT infrastructure	Organizations often have complex and interconnected IT infrastructures, consisting of various systems, applications, networks, and data centers. Managing the continuity of these diverse components and ensuring their seamless operation during a disruption can be challenging [153].
Rapidly evolving technology landscape	The IT landscape is constantly evolving, with new technologies, platforms, and frameworks being introduced regularly. Keeping up with these advancements and ensuring that the business continuity plan aligns with the changing technology landscape is a significant challenge [154].
Resource constraints	Developing and implementing an effective IT business continuity plan requires substantial resources, including financial, technological, and human resources. Limited budgets and resource constraints can hinder organizations from investing adequately in business continuity planning and preparedness activities [155].
Dependency on third-party service providers	Organizations often rely on third-party vendors and service providers for critical IT services [156]. Managing the risks associated with these dependencies, ensuring their preparedness for business continuity, and establishing effective communication and coordination mechanisms can be challenging.
Data protection and privacy	Organizations handle vast amounts of sensitive data, and ensuring its protection and privacy during a disruption is crucial [157], [158]. Implementing robust data backup, recovery, and security measures that comply with data protection regulations can be challenging, especially in the face of evolving threats and stringent privacy requirements.
Testing and exercising	Regular testing and exercising of the IT business continuity plan are essential to identify gaps, validate procedures, and improve response capabilities [159]. However, organizations often face challenges in conducting comprehensive testing due to operational limitations, resource constraints, or the fear of disrupting ongoing operations.
Human error and training	Human error can significantly impact the effectiveness of IT business continuity planning and response [160]. Providing adequate training to IT staff, creating awareness about their roles and responsibilities during a disruption, and conducting regular drills and simulations can help mitigate the risk of human error.
Changing regulatory and compliance landscape	Organizations must comply with various regulatory and compliance requirements related to data protection, privacy, and industry-specific regulations. Staying updated with changing regulations and ensuring that the IT business continuity plan aligns with these requirements can be a challenge [161].
Communication and coordination	During a disruption, effective communication and coordination among IT teams, business units, and stakeholders are critical [162]. Establishing clear lines of communication, defining roles and responsibilities, and ensuring smooth coordination across different teams and departments can be challenging, especially in large organizations.

6. Research gaps

While information technology (IT) disaster recovery planning and business continuity have been extensively studied, several research gaps still exist in this field. Some of the research gaps in IT disaster recovery planning and business continuity are discussed below:

Quantitative Metrics and Assessment: Developing robust quantitative metrics and assessment methodologies for evaluating the effectiveness and performance of IT disaster recovery plans and business continuity strategies [164] is a research gap. Establishing standardized metrics and measurement frameworks can help organizations objectively assess their preparedness, identify areas for improvement, and compare their performance with industry benchmarks. Figure 8 shows the plan-do-check-act model for IT disaster recovery.

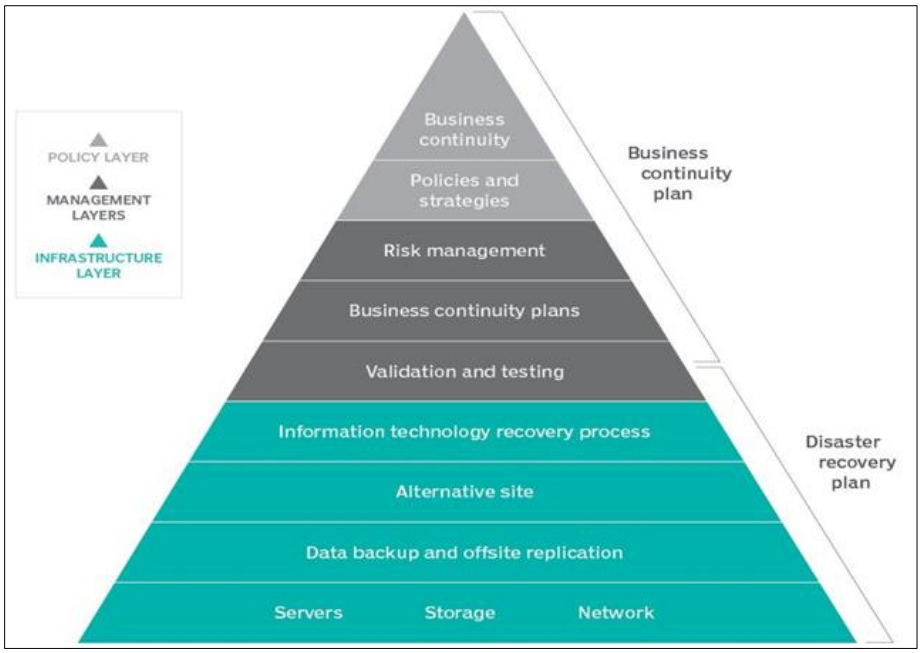

Figure 8 Model for Business continuity and IT disaster recovery planning

- *Cost-Effectiveness Analysis*: There is a need for research on cost-effectiveness analysis of IT disaster recovery planning and business continuity strategies. This includes evaluating the cost-benefit ratio of different recovery options, comparing the financial implications of various RTOs and RPOs [165], and determining the optimal allocation of resources [166] for IT recovery efforts.
- *Human-Centric Approaches*: Understanding the role of human factors in IT disaster recovery and business continuity [167] is a research gap. This includes studying factors such as decision-making under stress, the impact of organizational culture on recovery efforts, the role of leadership in driving resilience, and strategies for effectively managing the human element in IT recovery processes.
- *Cognitive Aspects*: Research on cognitive aspects, such as decision-making biases and cognitive biases [168] that may affect IT recovery processes, is limited. Investigating how cognitive biases influence decision-making during a crisis, and developing strategies to mitigate their impact, can enhance the effectiveness of IT disaster recovery planning and business continuity efforts.
- *Dynamic and Complex IT Environments*: The evolving IT landscape, characterized by dynamic and complex systems [169], poses challenges for IT disaster recovery planning and business continuity. Research can focus on developing strategies to address the complexities of distributed systems, virtualized environments, and cloud-based infrastructures, including efficient data synchronization, replication, and recovery mechanisms.
- *Cross-Organizational Collaboration*: Research on enhancing cross-organizational collaboration during IT disaster recovery [170] and business continuity is needed. Exploring mechanisms for effective information sharing, coordination, and collaboration between organizations, including public-private partnerships, can improve the overall resilience of interconnected IT ecosystems.
- *Cultural and Contextual Factors*: Cultural and contextual factors influence IT disaster recovery planning and business continuity practices [171]. Understanding how cultural values, organizational contexts, and regulatory frameworks impact IT recovery strategies and exploring approaches to tailor plans to specific cultural and contextual settings are areas for further research.
- *Cyber-security Considerations*: With the increasing frequency and sophistication of cyber threats [172], research on integrating cybersecurity considerations into IT disaster recovery planning and business continuity is crucial. This includes studying strategies for rapid incident response, cyber threat intelligence sharing, and recovery from cyber-attacks [173]-[176] to ensure the resilience of IT systems and protect organizational assets.
- *Artificial Intelligence and Automation*: The integration of artificial intelligence (AI) and automation in IT disaster recovery planning and business continuity is an emerging area that requires further research. Investigating the potential of AI-driven automation [177] for efficient monitoring, incident detection, and response can enhance the speed and accuracy of IT recovery processes.

Addressing these research gaps can contribute to the development of more effective IT disaster recovery plans and business continuity strategies, enabling organizations to better prepare for and recover from IT disruptions. It will also help organizations adapt to evolving technologies, emerging threats, and regulatory changes in the IT landscape.

7. Future research scope

Future research in information technology (IT) disaster recovery planning and business continuity can focus on several areas to address emerging challenges and advancements. The following are some potential research scopes that need to be explored.

- *Resilience in the Digital Age*: With the increasing reliance on digital technologies and interconnected systems [178], there is a need to study how organizations can build resilience in the face of emerging threats such as cyber-attacks, data breaches, and technological failures. Research can explore strategies to enhance IT infrastructure resilience, including secure backup and recovery mechanisms, advanced cybersecurity measures, and adaptive response strategies.
- *Cloud-Based Disaster Recovery*: As cloud computing continues to evolve [179], research can focus on developing effective disaster recovery strategies specific to cloud environments. This includes investigating cloud service provider selection criteria, assessing the reliability and availability of cloud services [180] for disaster recovery, and understanding the unique challenges and opportunities associated with leveraging cloud technology for business continuity.
- *Artificial Intelligence and Automation*: The integration of artificial intelligence (AI) and automation in disaster recovery planning and business continuity is an emerging area of research. Studying the use of AI-driven analytics, machine learning algorithms [181]-[185], and automation tools in risk assessment, decision-making, and response coordination can enhance the efficiency and effectiveness of IT recovery processes.
- *Internet of Things (IoT) Resilience*: As IoT devices become more prevalent in organizations [186], [187], understanding their vulnerabilities and developing resilience strategies is crucial. Research can focus on IoT device management, security protocols, and data protection mechanisms to ensure the resilience of IoT systems during and after a disaster.
- *Data Recovery and Integrity*: The increasing volume and complexity of data [188] pose challenges for effective data recovery and maintaining data integrity. Research can explore techniques and strategies for efficient data backup, restoration, and verification processes to ensure data availability and integrity in the event of a disaster.
- *Multi-Cloud and Hybrid Cloud Environments*: Organizations often operate in multi-cloud or hybrid cloud environments [189], combining public and private cloud services. Research can investigate the challenges and opportunities associated with designing and managing disaster recovery plans in such environments, including data synchronization, interoperability, and orchestration across multiple cloud platforms.
- *Human Factors and IT Recovery*: Understanding the role of human factors in IT recovery processes [190] is essential. Research can focus on factors such as decision-making under stress, teamwork and coordination, and training and awareness programs to improve the effectiveness of IT recovery efforts.
- *Regulatory Compliance and Legal Considerations*: The evolving regulatory landscape imposes various compliance requirements [191] on organizations regarding data privacy, security, and business continuity. Research can explore the legal and regulatory implications of IT disaster recovery planning and business continuity, addressing topics such as compliance frameworks, data protection laws, and liability issues.
- *Industry-Specific Considerations*: Different industries have unique IT requirements and regulatory landscapes [192]. Research can focus on industry-specific challenges and strategies for IT disaster recovery planning and business continuity in sectors such as healthcare, finance, manufacturing, and critical infrastructure.

By addressing these research scopes, organizations can stay abreast of emerging technologies, regulatory changes, and evolving threats, enabling them to develop more effective IT disaster recovery plans and business continuity strategies in the ever-evolving IT landscape. There is need to explore innovative approaches to enhance recovery capabilities, develop frameworks for integrating IT DRP and BC into the overall organizational risk management, investigate the resilience of emerging technologies, and conduct comprehensive assessments of the effectiveness and return on investment of different strategies. Additionally, research should also emphasize the importance of training and awareness programs, the role of communication and collaboration during recovery, and the alignment of IT DRP and BC with regulatory requirements and industry best practices.

8. Conclusion

IT disaster recovery planning and business continuity are indispensable elements of an organization's resilience strategy. They are vital for safeguarding IT systems, infrastructure, and services, as well as ensuring the continuity of critical business operations in the face of disruptive incidents or disasters. It has been shown that IT DRP focuses specifically on the recovery and restoration of IT capabilities, aiming to minimize downtime and data loss. It involves strategies, policies, and procedures that enable organizations to swiftly recover their IT infrastructure, systems, and services within predefined timeframes. This helps mitigate the impact of disruptions and facilitates a prompt return to normal operations. On the other hand, BC takes a broader perspective, encompassing the organization's ability to maintain essential operations and deliver critical services during and after a disruption. It includes not only the recovery of IT systems but also the coordination of various business functions, personnel, communication, and external stakeholders. BC ensures that the organization as a whole can effectively respond to and recover from disruptions, thereby preserving its reputation, customer trust, and revenue streams. The findings have indicated that implementing effective IT DRP and BC strategies is not without challenges. These include technological advancements, increasing system complexity, limited resources, organizational resistance, and the need for skilled personnel. Overcoming these challenges requires a holistic approach that involves thorough risk assessments, robust planning, and regular testing and maintenance of the plans. While extensive research has been conducted in the field of IT DRP and BC, there are still research gaps to address. These include the development of advanced recovery technologies, the integration of IT DRP and BC with overall risk management strategies, the impact of emerging technologies on recovery strategies, and the evaluation of the cost-effectiveness of different approaches. Future research should focus on bridging these gaps and exploring innovative solutions to enhance recovery capabilities, align IT DRP and BC with organizational risk management, and leverage emerging technologies for more efficient and resilient operations. Additionally, research should emphasize the importance of training and awareness, effective communication and collaboration, and compliance with regulatory requirements and industry standards.

Compliance with ethical standards

Acknowledgments

I would like to appreciate the efforts of all my colleagues who offered me support when writing this manuscript.

References

[1] Al Blooshi IA, Alamim AS, Said RA, Taleb N, Ghazal TM, Ahmad M, Alzoubi HM, Alshurideh M. IT Governance and Control: Mitigation and Disaster Preparedness of Organizations in the UAE. InThe Effect of Information Technology on Business and Marketing Intelligence Systems 2023 Feb 9 (pp. 661-677). Cham: Springer International Publishing.

[2] Bernanda DY, Charolina Y, Azhari O, Pangrestu C, Andry JF. identification of potential and planning for disaster recovery using the ISO/IEC 24762 standard at XYZ university. Jurnal Teknoinfo. 2023 Jan 1;17(1):140-7.

[3] Murodilov KT. Use of geo-information systems for monitoring and development of the basis of web-maps. Galaxy International Interdisciplinary Research Journal. 2023 Apr 20, 11(4):685-9.

[4] Roztocki N, Strzelczyk W, Weistroffer HR. The role of e-government in disaster management: A review of the literature. Journal of Economics and Management. 2023 Jan 1, 45(1):1-25.

[5] Abid SK, Sulaiman N, Wei CS, Nazir U. Building resilient future: Information technology and disaster management-a Malaysian perspective. InIOP Conference Series: Earth and Environmental Science 2021 Jun 1 (Vol. 795, No. 1, p. 012026). IOP Publishing.

[6] Hussien ZA, Abdulmalik HA, Hussain MA, Nyangaresi VO, Ma J, Abduljabbar ZA, Abduljaleel IQ. Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems. Applied Sciences. 2023 Jan, 13(2):691.

[7] Aleksandrova SV, Aleksandrov MN, Vasiliev VA. Business continuity management system. In2018 IEEE International Conference" Quality Management, Transport and Information Security, Information Technologies"(IT&QM&IS) 2018 Sep 24 (pp. 14-17). IEEE.

[8] Zare H, Wang P, Zare MJ, Azadi M, Olsen P. Business Continuity Plan and Risk Assessment Analysis in Case of a Cyber Attack Disaster in Healthcare Organizations. In17th International conference on information technology–new generations (ITNG 2020) 2020 (pp. 137-144). Springer International Publishing.

[9] Budiman K, Arini FY, Sugiharti E. Disaster recovery planning with distributed replicated block device in synchronized API systems. InJournal of Physics: Conference Series 2020 Jun 1 (Vol. 1567, No. 3, p. 032023). IOP Publishing.

[10] Ratnasari A, Fitrianah D, Haji WH. BPTrends Redesign Methodology (BPRM) for the Development Disaster Management Prevention Information System. InProceedings of the 2020 2nd Asia Pacific Information Technology Conference 2020 Jan 17 (pp. 113-117).

[11] Meechang K, Leelawat N, Tang J, Kodaka A, Chintanapakdee C. The acceptance of using information technology for disaster risk management: A systematic review. Engineering Journal. 2020 Jul 31, 24(4):111-32.

[12] Nyangaresi VO. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks. 2023 Apr 1, 142:103117.

[13] Ashrafi R, AlKindi H. A framework for IS/IT disaster recovery planning. International Journal of Business Continuity and Risk Management. 2022, 12(1):1-21.

[14] Corallo A, Lazoi M, Lezzi M. Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. Computers in industry. 2020 Jan 1, 114:103165.

[15] Hassel H, Cedergren A. Integrating risk assessment and business impact assessment in the public crisis management sector. International Journal of Disaster Risk Reduction. 2021 Apr 1, 56:102136.

[16] Möller DP. Ransomware Attacks and Scenarios: Cost Factors and Loss of Reputation. InGuide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices 2023 Apr 19 (pp. 273-303). Cham: Springer Nature Switzerland.

[17] Al Sibahee MA, Nyangaresi VO, Ma J, Abduljabbar ZA. Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things. InInternational Conference on Internet of Things as a Service 2021 Dec 13 (pp. 3-18). Cham: Springer International Publishing.

[18] Hamadah S, Aqel D. A proposed virtual private cloud-based disaster recovery strategy. In2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT) 2019 Apr 9 (pp. 469-473). IEEE.

[19] Manupati VK, Schoenherr T, Ramkumar M, Panigrahi S, Sharma Y, Mishra P. Recovery strategies for a disrupted supply chain network: Leveraging blockchain technology in pre-and post-disruption scenarios. International Journal of Production Economics. 2022 Mar 1, 245:108389.

[20] Swagatika S, Panda N. Cloud-based backup and data recovery. Journal of Information and Optimization Sciences. 2022 Jul 4, 43(5):923-32.

[21] Logeshwaran J, Ramesh G, Aravindarajan V. A secured database monitoring method to improve data backup and recovery operations in cloud computing. BOHR International Journal of Computer Science. 2023 Feb 8, 2(1):1-7.

[22] Zhang Y, Xu C, Muntean GM. A Novel Distributed Data Backup and Recovery Method for Software Defined-WAN Controllers. In2021 IEEE Global Communications Conference (GLOBECOM) 2021 Dec 7 (pp. 01-06). IEEE.

[23] Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Spatial single mode laser source interaction with measured pulse based parabolic index multimode fiber. Journal of Optical Communications. 2022 Jun 21.

[24] Prasetyo HN, Supriatna N, Raharjo AP, Wikusna W. Information technology disaster recovery plan (IT-DRP) model-based on NIST framework in Indonesia. IJAIT (International Journal of Applied Information Technology). 2019:34-45.

[25] Anthoniraj S, Saraswathi S. Frequent failure monitoring and reporting in virtualisation environment using backing algorithm technique. International Journal of Information and Communication Technology. 2018, 12(1-2):131-42.

[26] Hu P. Computer testing and maintenance and data recovery technology. InJournal of Physics: Conference Series 2020 Oct 1 (Vol. 1648, No. 2, p. 022198). IOP Publishing.

[27] Izonin I, Kryvinska N, Tkachenko R, Zub K. An approach towards missing data recovery within IoT smart system. Procedia Computer Science. 2019 Jan 1, 155:11-8.

[28] Almaqtari FA, Farhan NH, Al-Hattami HM, Elsheikh T. The moderating role of information technology governance in the relationship between board characteristics and continuity management during the Covid-19 pandemic in an emerging economy. Humanities and Social Sciences Communications. 2023 Mar 10, 10(1):1-6.

[29] Assibi AT. Literature Review on Building Cyber Resilience Capabilities to Counter Future Cyber Threats: The Role of Enterprise Risk Management (ERM) and Business Continuity (BC). Open Access Library Journal. 2023 Apr 4, 10(4):1-5.

[30] Nyangaresi VO, Ma J. A Formally Verified Message Validation Protocol for Intelligent IoT E-Health Systems. In2022 IEEE World Conference on Applied Intelligence and Computing (AIC) 2022 Jun 17 (pp. 416-422). IEEE.

[31] Mejri O, Menoni S, Matias K, Aminoltaheri N. Crisis information to support spatial planning in post disaster recovery. International journal of disaster risk reduction. 2017 Jun 1, 22:46-61.

[32] Zhao C, Ding D, Du Z, Shi Y, Su G, Yu S. Analysis of perception accuracy of roadside millimeter-wave radar for traffic risk assessment and early warning systems. International journal of environmental research and public health. 2023 Jan 3, 20(1):879.

[33] Peng Y, Welden N, Renaud FG. A framework for integrating ecosystem services indicators into vulnerability and risk assessments of deltaic social-ecological systems. Journal of Environmental Management. 2023 Jan 15, 326:116682.

[34] Aghabegloo M, Rezaie K, Torabi SA, Khalili SM. A BIA-Based Quantitative Framework for Built Physical Asset Criticality Analysis under Sustainability and Resilience. Buildings. 2023 Jan 16, 13(1):264.

[35] Klein J. Paying for community pharmacy-based medication reviews for Type 2 Diabetes: A feasibility and budget impact analysis (Doctoral dissertation, Hochschule für Angewandte Wissenschaften Hamburg).

[36] Tamimi AA, Dawood R, Sadaqa L. Disaster recovery techniques in cloud computing. In2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT) 2019 Apr 9 (pp. 845-850). IEEE.

[37] Qiu Z, Ma J, Zhang H, Al Sibahee MA, Abduljabbar ZA, Nyangaresi VO. Concurrent pipeline rendering scheme based on GPU multi-queue and partitioning images. InInternational Conference on Optics and Machine Vision (ICOMV 2023) 2023 Apr 14 (Vol. 12634, pp. 143-149). SPIE.

[38] Sharma A, Trivedi A, Srinivasan D. Multi-stage restoration strategy for service restoration in distribution systems considering outage duration uncertainty. IET Generation, Transmission & Distribution. 2018 Oct, 12(19):4319-26.

[39] Swain AK, Garza VR. Key factors in achieving Service Level Agreements (SLA) for Information Technology (IT) incident resolution. Information Systems Frontiers. 2023 Apr, 25(2):819-34.

[40] Amini M, Rahmani A. How Strategic Agility Affects the Competitive Capabilities of Private Banks. International Journal of Basic and Applied Sciences. 2023, 10:8397-406.

[41] Fotis G, Vita V, Maris TI. Risks in the European Transmission System and a Novel Restoration Strategy for a Power System after a Major Blackout. Applied Sciences. 2023 Jan, 13(1):83.

[42] Edib SN, Lin Y, Vokkarane VM, Qiu F, Yao R, Chen B. Cyber Restoration of Power Systems: Concept and Methodology for Resilient Observability. IEEE Transactions on Systems, Man, and Cybernetics: Systems. 2023 Apr 24.

[43] Nyangaresi VO. Extended Chebyshev Chaotic Map Based Message Verification Protocol for Wireless Surveillance Systems. InComputer Vision and Robotics: Proceedings of CVR 2022 2023 Apr 28 (pp. 503-516). Singapore: Springer Nature Singapore.

[44] Gamoura SC. A Cloud-Based Approach for Cross-Management of Disaster Plans: Managing Risk in Networked Enterprises. InEmergency and Disaster Management: Concepts, Methodologies, Tools, and Applications 2019 (pp. 857-881). IGI Global.

[45] Sakurai M, Murayama Y. Information technologies and disaster management–Benefits and issues. Progress in Disaster Science. 2019 Jul 1, 2:100012.

[46] Samsudin K, Ghazali FN, Abdul Ghani NH, Hussin MF, Kamarudin AH, Kasri H. Effective Emergency Management: Scrutinizing the Malaysia Lead Responding Agency Planning and Information Management Approach During Disaster Exercise. Pertanika Journal of Science & Technology. 2022 Oct 1, 30(4):2521-34.

[47] Frith KH. Information Technology Systems Continuity Plan. Nursing Education Perspectives. 2022 Sep 1, 43(5):337.

[48] Munawar HS, Mojtahedi M, Hammad AW, Kouzani A, Mahmud MP. Disruptive technologies as a solution for disaster risk management: A review. Science of the total environment. 2022 Feb 1, 806:151351.

[49] Al-Chaab W, Abduljabbar ZA, Abood EW, Nyangaresi VO, Mohammed HM, Ma J. Secure and Low-Complexity Medical Image Exchange Based on Compressive Sensing and LSB Audio Steganography. Informatica. 2023 May 31, 47(6).

[50] Doel T, Shakir DI, Pratt R, Aertsen M, Moggridge J, Bellon E, David AL, Deprest J, Vercauteren T, Ourselin S. GIFT-Cloud: A data sharing and collaboration platform for medical imaging research. computer methods and programs in biomedicine. 2017 Feb 1, 139:181-90.

[51] Thomas J, Galligher G. Improving backup system evaluations in information security risk assessments to combat ransomware. Computer and Information Science. 2018, 11(1).

[52] Guan S, Zhang C, Wang Y, Liu W. Hadoop-based secure storage solution for big data in cloud computing environment. Digital Communications and Networks. 2023 Jan 20.

[53] Farid G, Warraich NF, Iftikhar S. Digital information security management policy in academic libraries: A systematic review (2010–2022). Journal of Information Science. 2023 Apr 5:01655515231160026.

[54] Bandari V. Enterprise Data Security Measures: A Comparative Review of Effectiveness and Risks Across Different Industries and Organization Types. International Journal of Business Intelligence and Big Data Analytics. 2023 Jan 20, 6(1):1-1.

[55] Nyangaresi VO, Moundounga AR. Secure data exchange scheme for smart grids. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 312-316). IEEE.

[56] Rajić MN, Maksimović RM, Milosavljević P. Emergency Planning and Disaster Recovery Management Model in Hospitality—Plan-Do-Check-Act Cycle Approach. Sustainability. 2023 Apr 6, 15(7):6303.

[57] Sharif SV, Moshfegh PH, Kashani H. Simulation modeling of operation and coordination of agencies involved in post-disaster response and recovery. Reliability Engineering & System Safety. 2023 Jul 1, 235:109219.

[58] Schwarz K, Aranda DA, Hartmann M. Towards Automated Situational Awareness Reporting for Disaster Management—A Case Study. Sustainability. 2023 May 13, 15(10):7968.

[59] Johnson R, McIntosh C, Tropasso C. Deploying Modern Technology for Disaster Management Practitioners. InDisaster Management and Information Technology: Professional Response and Recovery Management in the Age of Disasters 2023 Apr 1 (pp. 25-34). Cham: Springer International Publishing.

[60] Wong R, Morris K, Masys AJ. Exercises to Support Safety and Security. InSafety and Security Science and Technology: Perspectives from Practice 2023 Mar 1 (pp. 127-139). Cham: Springer International Publishing.

[61] Abduljabbar ZA, Omollo Nyangaresi V, Al Sibahee MA, Ghrabat MJ, Ma J, Qays Abduljaleel I, Aldarwish AJ. Session-Dependent Token-Based Payload Enciphering Scheme for Integrity Enhancements in Wireless Networks. Journal of Sensor and Actuator Networks. 2022 Sep 19, 11(3):55.

[62] Tropp EM, Hoffmann T, Chochia A. Open Data: A Stepchild in e-Estonia's Data Management Strategy?. TalTech Journal of European Studies. 2022, 12(1):123-44.

[63] Djoumessi YF, Mbongo LD. An analysis of information communication technologies for natural disaster management in Africa. International Journal of Disaster Risk Reduction. 2022 Jan 1, 68:102722.

[64] Rak J, Girao-Silva R, Gomes T, Ellinas G, Kantarci B, Tornatore M. Disaster resilience of optical networks: State of the art, challenges, and opportunities. Optical Switching and Networking. 2021 Nov 1, 42:100619.

[65] Liu H, Tatano H, Samaddar S. Analysis of post-disaster business recovery: Differences in industrial sectors and impacts of production inputs. International Journal of Disaster Risk Reduction. 2023 Mar 1, 87:103577.

[66] Joo MR, Sinha R. Performance-based selection of pathways for enhancing built infrastructure resilience. Sustainable and Resilient Infrastructure. 2023 Mar 12:1-23.

[67] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432). IEEE.

[68] Perumal K, Mohan S, Frnda J, Divakarachari PB. Dynamic resource provisioning and secured file sharing using virtualization in cloud azure. Journal of Cloud Computing. 2022 Dec, 11(1):1-2.

[69] Salagrama S, Bibhu V. Study of IT and Data Center Virtualization. In2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM) 2022 Feb 23 (Vol. 2, pp. 274-278). IEEE.

[70] Adoga HU, Pezaros DP. Network function virtualization and service function chaining frameworks: A comprehensive review of requirements, objectives, implementations, and open research challenges. Future Internet. 2022 Feb 15, 14(2):59.

[71] Gupta N, Gupta K, Gupta D, Juneja S, Turabieh H, Dhiman G, Kautish S, Viriyasitavat W. Enhanced virtualization-based dynamic bin-packing optimized energy management solution for heterogeneous clouds. Mathematical Problems in Engineering. 2022 Jan 30, 2022.

[72] Yaqoob I, Salah K, Jayaraman R, Al-Hammadi Y. Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Computing and Applications. 2021 Jan 7:1-6.

[73] Attaran M, Woods J. Cloud computing technology: improving small business performance using the Internet. Journal of Small Business & Entrepreneurship. 2019 Nov 2, 31(6):495-519.

[74] Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Khalefa MS, Honi DG. MAC-Based Symmetric Key Protocol for Secure Traffic Forwarding in Drones. InFuture Access Enablers for Ubiquitous and Intelligent Infrastructures: 6th EAI International Conference, FABULOUS 2022, Virtual Event, May 4, 2022, Proceedings 2022 Sep 18 (pp. 16-36). Cham: Springer International Publishing.

[75] Liao YK, Wu CY, Truong GN, Do YT. The Roles of Service Recovery and Perceived Justice on Post-Recovery Satisfaction in M-Commerce. Sustainability. 2022 Nov 10, 14(22):14838.

[76] Murphy B, Pearce L, Chretien A, McLean-Purdon E. Mutual Aid and Service Agreements: Wise Practices for First Nations Communities.

[77] Switzer D, Wang W, Hirschvogel L. Municipal utilities and COVID-19: Challenges, responses, and collaboration. The American Review of Public Administration. 2020 Aug, 50(6-7):577-83.

[78] Johnson GA, Shriver SK, Goldberg SG. Privacy and market concentration: intended and unintended consequences of the GDPR. Management Science. 2023 Mar 10.

[79] Nandankar S, Sachan A, Adhikari A, Mukherjee A. Developing and validating e-marketplace service quality model in B2G e-commerce settings: a mixed-methods approach. International Journal of Operations & Production Management. 2023 Mar 9.

[80] bin Salleh R, Koubaa A, Khan Z, Khan MK, Ali I. Data plane failure and its recovery techniques in SDN: A systematic literature review. Journal of King Saud University-Computer and Information Sciences. 2023 Feb 11.

[81] Nyangaresi VO, Ogundoyin SO. Certificate based authentication scheme for smart homes. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 202-207). IEEE.

[82] Deymi-Dashtebayaz M, Valipour-Namanlo S. Thermoeconomic and environmental feasibility of waste heat recovery of a data center using air source heat pump. Journal of Cleaner Production. 2019 May 10, 219:117-26.

[83] Huang Y, Deng Z, Chen Y, Zhang C. Performance investigation of a biomimetic latent heat thermal energy storage device for waste heat recovery in data centers. Applied Energy. 2023 Apr 1, 335:120745.

[84] Zhang Y, Shan K, Li X, Li H, Wang S. Research and Technologies for next-generation high-temperature data centers–State-of-the-arts and future perspectives. Renewable and Sustainable Energy Reviews. 2023 Jan 1, 171:112991.

[85] Civča D, Atstāja D, Koval V. Business continuity plan testing methods in an international company. Restruct. Manag. Increase Compet. Trading Co. Latv. 2021, 5:341.

[86] Ellitan L, Anatan L. Achieving business continuity in Industrial 4.0 and Society 5.0. International Journal of Trend in Scientific Research and Development (IJTSRD). 2020 Feb, 4(2):235-9.

[87] Alsamhi SH, Shvetsov AV, Kumar S, Shvetsova SV, Alhartomi MA, Hawbani A, Rajput NS, Srivastava S, Saif A, Nyangaresi VO. UAV computing-assisted search and rescue mission framework for disaster and harsh environment mitigation. Drones. 2022 Jun 22, 6(7):154.

[88] Charoenthammachoke K, Leelawat N, Tang J, Kodaka A. Business continuity management: A preliminary systematic literature review based on ScienceDirect database. Journal of disaster research. 2020 Aug 1, 15(5):546-55.

[89] Fani SV, Subriadi AP. Business continuity plan: examining of multi-usable framework. Procedia Computer Science. 2019 Jan 1, 161:275-82.

[90] Miao M, Saide S, Ratna S, Muflih M. Business continuity innovation in disruption time: Sociotechnical systems, business analytics, virtual business, and mediating role of knowledge absorptive capacity. IEEE Transactions on Engineering Management. 2021 Jul 5.

[91] Taherdoost H. A review on risk management in information systems: Risk policy, control and fraud detection. Electronics. 2021 Jan, 10(24):3065.

[92] Kure HI, Islam S. Assets focus risk management framework for critical infrastructure cybersecurity risk management. IET Cyber-Physical Systems: Theory & Applications. 2019 Dec, 4(4):332-40.

[93] Nyangaresi VO, Morsy MA. Towards privacy preservation in internet of drones. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[94] Bahşi H, Udokwu CJ, Tatar U, Norta A. Impact assessment of cyber actions on missions or business processes: A systematic literature review. InICCWS 2018 13th International Conference on Cyber Warfare and Security 2018 Mar 8 (p. 11). Academic Conferences and publishing limited.

[95] Labus M, Despotović-Zrakić M, Bogdanović Z, Barać D, Popović S. Adaptive e-business continuity management: Evidence from the financial sector. Computer Science and Information Systems. 2020, 17(2):553-80.

[96] Rezaei Soufi H, Torabi SA, Sahebjamnia N. Developing a novel quantitative framework for business continuity planning. International Journal of Production Research. 2019 Feb 1, 57(3):779-800.

[97] Wang Q. Cloud Data Backup and Recovery Method Based on the DELTA Compression Algorithm. In2021 IEEE International Conference on Industrial Application of Artificial Intelligence (IAAI) 2021 Dec 24 (pp. 183-188). IEEE.

[98] Fathima Nifra N, Razeeth S. Database backup and recovery: a review with test implementation for MYSQL and NOSQL databases.

[99] Nyakomitta PS, Nyangaresi VO, Ogara SO. Efficient authentication algorithm for secure remote access in wireless sensor networks. Journal of Computer Science Research. 2021 Aug, 3(4):43-50.

[100] Sawalha IH. Business continuity management: use and approach's effectiveness. Continuity & Resilience Review. 2020 Sep 4, 2(2):81-96.

[101] Vanichchinchai A. Links between components of business continuity management: an implementation perspective. Business Process Management Journal. 2023 Jan 9(ahead-of-print).

[102] Abdulhameed AA, Al-Kubaisy SA. The Effect of Knowledge Upgrading on Business Continuity: A Field Research in Private Colleges and Universities in Baghdad. Journal of Economics and Administrative Sciences. 2023 Jun 5, 29(136):1-5.

[103] Kato M, Charoenrat T. Business continuity management of small and medium sized enterprises: Evidence from Thailand. International journal of disaster risk reduction. 2018 Mar 1, 27:577-87.

[104] Păunescu C, Argatu R. Critical functions in ensuring effective business continuity management. Evidence from Romanian companies. Journal of Business Economics and Management. 2020 Mar 26, 21(2):497-520.

[105] Nyangaresi VO, Petrovic N. Efficient PUF based authentication protocol for internet of drones. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[106] Tarigan ZJ, Suprapto W, Harjanti D, Malelak MI, Basana SR. Key user ERP capability maintaining ERP sustainability through effective design of business process and integration data management Key user ERP capability maintaining ERP sustainability through effective design of business process and integration data management (Doctoral dissertation, Petra Christian University).

[107] Romancheva NI. Using edge service for secure information systems availability. InAIP Conference Proceedings 2023 Mar 9 (Vol. 2700, No. 1, p. 040041). AIP Publishing LLC.

[108] Ardolino F, Parrillo F, Di Domenico C, Costarella F, Arena U. Combined Use of an Information System and LCA Approach to Assess the Performances of a Solid Waste Management System. Applied Sciences. 2023 Jan 4, 13(2):707.

[109] Rasoulian S, Grégoire Y, Legoux R, Sénécal S. The effects of service crises and recovery resources on market reactions: An event study analysis on data breach announcements. Journal of Service Research. 2023 Feb, 26(1):44-63.

[110] Khanum S, Mustafa K. A systematic literature review on sensitive data protection in blockchain applications. Concurrency and Computation: Practice and Experience. 2023 Jan 10, 35(1):e7422.

[111] Goel L, Russell D, Williamson S, Zhang JZ. Information systems security resilience as a dynamic capability. Journal of Enterprise Information Management. 2023 Feb 28.

[112] Al Sibahee MA, Abdulsada AI, Abduljabbar ZA, Ma J, Nyangaresi VO, Umran SM. Lightweight, Secure, Similar-Document Retrieval over Encrypted Data. Applied Sciences. 2021 Jan, 11(24):12040.

[113] Bitzer M, Häckel B, Leuthe D, Ott J, Stahl B, Strobel J. Managing the Inevitable–A Maturity Model to Establish Incident Response Management Capabilities. Computers & Security. 2023 Feb 1., 125:103050.

[114] Woods DW, Böhme R, Wolff J, Schwarcz D. Lessons lost: incident response in the age of cyber insurance and breach attorneys. InProceedings of the 32nd USENIX Security Symposium 2023.

[115] Serrano MA, Sánchez LE, Santos-Olmo A, García-Rosado D, Blanco C, Barletta VS, Caivano D, Fernández-Medina E. Minimizing incident response time in real-world scenarios using quantum computing. Software Quality Journal. 2023 May 26:1-30.

[116] Riebe T, Bäumler J, Kaufhold MA, Reuter C. Values and Value Conflicts in the Context of OSINT Technologies for Cybersecurity Incident Response: A Value Sensitive Design Perspective. Computer Supported Cooperative Work (CSCW). 2023 Apr 4:1-47.

[117] Chatterjee S, Chaudhari R, Shams R. Applications of Industry 4.0 for Pandemic Responses and Business Continuity: A TOE-DCV Integrated Approach. IEEE Transactions on Engineering Management. 2023 Mar 17.

[118] Deretarla Ö, Erdebilli B, Gündoğan M. An integrated Analytic Hierarchy Process and Complex Proportional Assessment for vendor selection in supply chain management. Decision Analytics Journal. 2023 Mar 1, 6:100155.

[119] Nyangaresi VO. Target Tracking Area Selection and Handover Security in Cellular Networks: A Machine Learning Approach. InProceedings of Third International Conference on Sustainable Expert Systems: ICSES 2022 2023 Feb 23 (pp. 797-816). Singapore: Springer Nature Singapore.

[120] Pantos S. Designing Stress Tests for UK Fast-Growing Firms and Fintech. Risks. 2023 Jan 31, 11(2):31.

[121] Trifonova N, Proshkina A, Bezrukov A, Korolev A, Paren A. Sustainability and Business Continuity Management for Production System in the Energy Sector in the Face of Increasing Uncertainty and Risk: Who Determines?. InInternational Scientific and Practical Conference" Young Engineers of the Fuel and Energy Complex: Developing the Energy Agenda of the Future"(EAF 2021) 2022 Mar 24 (pp. 173-177). Atlantis Press.

[122] Fernando MS. IT disaster recovery system to ensure the business continuity of an organization. In2017 National Information Technology Conference (NITC) 2017 Sep 14 (pp. 46-48). IEEE.

[123] Moşteanu DN. Management of disaster and business continuity in a digital world. International Journal of Management. 2020 May 14, 11(4).

[124] Vanichchinchai A. The influences of organizational contexts on business continuity management. Business Process Management Journal. 2023 Jan 13, 29(1):100-15.

[125] Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA, Nyangaresi VO, Honi DG, Abdulsada AI, Jiao X. Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map. IEEE Access. 2022 Feb 11, 10:26257-70.

[126] Naim MH, Zain JM, Abd Jalil K. Fault Tolerance Mechanism for Software Application Through Fog Computing as Middleware. International Journal of Computing and Digital Systems. 2022 Feb 15, 11(1):45-54.

[127] Zhang Y, Zhong L, Yang S, Muntean GM. Distributed data backup and recovery for software-defined wide area network controllers. Transactions on Emerging Telecommunications Technologies. 2022 Apr, 33(4):e4411.

[128] Borangiu T, Trentesaux D, Thomas A, Leitão P, Barata J. Digital transformation of manufacturing through cloud services and resource virtualization. Computers in Industry. 2019 Jun 1, 108:150-62.

[129] Tabassum N, Ditta A, Alyas T, Abbas S, Alquhayz H, Mian NA, Khan MA. Prediction of cloud ranking in a hyperconverged cloud ecosystem using machine learning.

[130] Duan Q. Cloud service performance evaluation: status, challenges, and opportunities–a survey from the system modeling perspective. Digital Communications and Networks. 2017 May 1, 3(2):101-11.

[131] Nyangaresi VO, Abood EW, Abduljabbar ZA, Al Sibahe MA. Energy Efficient WSN Sink-Cloud Server Authentication Protocol. In2021 5th International Conference on Information Systems and Computer Networks (ISCON) 2021 Oct 22 (pp. 1-6).

[132] Malecki F. Now is the time to move past traditional 3-2-1 back-ups. Network Security. 2021 Jan 1, 2021(1):18-9.

[133] Ahmad A, Maynard SB, Desouza KC, Kotsias J, Whitty MT, Baskerville RL. How can organizations develop situation awareness for incident response: A case study of management practice. Computers & Security. 2021 Feb 1, 101:102122.

[134] Shinde N, Kulkarni P. Cyber incident response and planning: a flexible approach. Computer Fraud & Security. 2021 Jan, 2021(1):14-9.

[135] Sawalha IH. Views on business continuity and disaster recovery. International Journal of Emergency Services. 2021 May 25, 10(3):351-65.

[136] Panevski V. Possible integrity framework between the Intelligent Security Systems parameters and the Business Continuity Management processes. Security & Future. 2021, 5(2):42-5.

[137] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA. Symmetric Key Based Scheme for Verification Token Generation in Internet of Things Communication Environment. InApplied Cryptography in Computer and Communications: Second EAI International Conference, AC3 2022, Virtual Event, May 14-15, 2022, Proceedings 2022 Oct 6 (pp. 46-64). Cham: Springer Nature Switzerland.

[138] Modgil S, Singh RK, Hannibal C. Artificial intelligence for supply chain resilience: learning from Covid-19. The International Journal of Logistics Management. 2022 Oct 17, 33(4):1246-68.

[139] Phillips R, Tanner B. Breaking down silos between business continuity and cyber security. Journal of business continuity & emergency planning. 2019 Jan 1, 12(3):224-32.

[140] Settanni G, Skopik F, Shovgenya Y, Fiedler R, Carolan M, Conroy D, Boettinger K, Gall M, Brost G, Ponchel C, Haustein M. A collaborative cyber incident management system for European interconnected critical infrastructures. Journal of Information Security and Applications. 2017 Jun 1, 34:166-82.

[141] Aanestad M, Grisot M, Hanseth O, Vassilakopoulou P. Information infrastructures and the challenge of the installed base. Information infrastructures within European health care: Working with the installed base. 2017:25-33.

[142] Iqbal Z, Sadaf S. Forty years of directed evolution and its continuously evolving technology toolbox: A review of the patent landscape. Biotechnology and Bioengineering. 2022 Mar, 119(3):693-724.

[143] Alzahrani A, Alyas T, Alissa K, Abbas Q, Alsaawy Y, Tabassum N. Hybrid Approach for Improving the Performance of Data Reliability in Cloud Storage Management. Sensors. 2022 Aug 10, 22(16):5966.

[144] Hussain MA, Hussien ZA, Abduljabbar ZA, Ma J, Al Sibahee MA, Hussain SA, Nyangaresi VO, Jiao X. Provably throttling SQLI using an enciphering query and secure matching. Egyptian Informatics Journal. 2022 Dec 1, 23(4):145-62.

[145] Andrade E, Nogueira B. Dependability evaluation of a disaster recovery solution for IoT infrastructures. The Journal of Supercomputing. 2020 Mar, 76(3):1828-49.

[146] Mendonça J, Lima R, Andrade E, Araujo J, Kim DS. Multiple-criteria Evaluation of Disaster Recovery Strategies Based on Stochastic Models. In2020 16th International Conference on the Design of Reliable Communication Networks DRCN 2020 2020 Mar 25 (pp. 1-7). IEEE.

[147] Sheykhmousa M, Kerle N, Kuffer M, Ghaffarian S. Post-disaster recovery assessment with machine learning-derived land cover and land use information. Remote sensing. 2019 May 17, 11(10):1174.

[148] Al-Balushi Z, Durugbo CM. Management strategies for supply risk dependencies: empirical evidence from the gulf region. International Journal of Physical Distribution & Logistics Management. 2020 May 19, 50(4):457-81.

[149] Shanker S, Sharma H, Barve A. Analysing the critical success factors and the risks associated with third-party logistics in the food supply chain: a case of coffee industry. Journal of Advances in Management Research. 2022 Apr 1, 19(2):161-97.

[150] Nyangaresi VO, Alsamhi SH. Towards secure traffic signaling in smart grids. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 196-201). IEEE.

[151] Negi S, Negi G. Framework to manage humanitarian logistics in disaster relief supply chain management in India. International Journal of Emergency Services. 2021 Apr 6, 10(1):40-76.

[152] Grundstrom C, Väyrynen K, Iivari N, Isomursu M. Making sense of the general data protection regulation—four categories of personal data access challenges.

[153] Xiahou X, Chen J, Zhao B, Yan Z, Cui P, Li Q, Yu Z. Research on Safety Resilience Evaluation Model of Data Center Physical Infrastructure: An ANP-Based Approach. Buildings. 2022 Nov 7, 12(11):1911.

[154] Atzori L, Iera A, Morabito G. Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm. Ad Hoc Networks. 2017 Mar 1, 56:122-40.

[155] Ghaderi Z, King B, Hall CM. Crisis preparedness of hospitality managers: evidence from Malaysia. Journal of Hospitality and Tourism Insights. 2022 Apr 6, 5(2):292-310.

[156] Topping C, Dwyer A, Michalec O, Craggs B, Rashid A. Beware suppliers bearing gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks. Computers & Security. 2021 Sep 1, 108:102324.

[157] Galetsi P, Katsaliaki K, Kumar S. Values, challenges and future directions of big data analytics in healthcare: A systematic review. Social science & medicine. 2019 Nov 1, 241:112533.

[158] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Sep 1, 15:100210.

[159] Groenendaal J, Helsloot I. Organisational resilience: Shifting from planning-driven business continuity management to anticipated improvisation. Journal of Business Continuity & Emergency Planning. 2020 Jan 1, 14(2):102-9.

[160] Gracey A, Yearwood K. Building an effective business continuity framework: Case study of a critical national infrastructure organisation's approach. Journal of Business Continuity & Emergency Planning. 2022 Jan 1, 15(4):342-59.

[161] Klievink B, Janssen M, van Der Voort H, Van Engelenburg S. Regulatory compliance and over-compliant information sharing–changes in the B2G landscape. InElectronic Government: 17th IFIP WG 8.5 International Conference, EGOV 2018, Krems, Austria, September 3-5, 2018, Proceedings 17 2018 (pp. 249-260). Springer International Publishing.

[162] Monstadt J, Schmidt M. Urban resilience in the making? The governance of critical infrastructures in German cities. Urban Studies. 2019 Aug, 56(11):2353-71.

[163] Chiossi S, Tsolova S, Ciotti M. Assessing public health emergency preparedness: a scoping review on recent tools and methods. International Journal of Disaster Risk Reduction. 2021 Apr 1, 56:102104.

[164] Russo N, Reis L, Silveira C, Mamede HS. Towards a Comprehensive Framework for the Multidisciplinary Evaluation of Organizational Maturity on Business Continuity Program Management: A Systematic Literature Review. Information Security Journal: A Global Perspective. 2023 Mar 29:1-9.

[165] Mendonça J, Lima R, Queiroz E, Andrade E, Kim DS. Evaluation of a backup-as-a-service environment for disaster recovery. In2019 IEEE Symposium on Computers and Communications (ISCC) 2019 Jun 29 (pp. 1-6). IEEE.

[166] Abood EW, Hussien ZA, Kawi HA, Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Kalafy A, Ahmad S. Provably secure and efficient audio compression based on compressive sensing. International Journal of Electrical & Computer Engineering (2088-8708). 2023 Feb 1, 13(1).

[167] Hamid AH. Limitations and challenges towards an effective business continuity management in Nuklear Malaysia. InIOP conference series: materials science and engineering 2018 (Vol. 298, No. 1, p. 012050). IOP Publishing.

[168] Acciarini C, Brunetta F, Boccardelli P. Cognitive biases and decision-making strategies in times of change: a systematic literature review. Management Decision. 2021 May 4, 59(3):638-52.

[169] Ruijer E, Dingelstad J, Meijer A. Studying complex systems through design interventions probing open government data ecosystems in the Netherlands. Public Management Review. 2023 Jan 2, 25(1):129-49.

[170] Wu Q, Zhu J, Cheng Y. The effect of cross-organizational governance on supply chain resilience: A mediating and moderating model. Journal of Purchasing and Supply Management. 2023 Jan 1, 29(1):100817.

[171] Naser AF, Nor A. The The Mediating Effect of Disaster Recovery Plan on the Relationship Between Critical Personnel And Business Continuity Management. International Journal of Business, Management and Economics. 2022 Nov 17, 3(4):382-400.

[172] Nyangaresi VO. Hardware assisted protocol for attacks prevention in ad hoc networks. InEmerging Technologies in Computing: 4th EAI/IAER International Conference, iCETiC 2021, Virtual Event, August 18–19, 2021, Proceedings 4 2021 (pp. 3-20). Springer International Publishing.

[173] Tounsi W, Rais H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & security. 2018 Jan 1, 72:212-33.

[174] Nitz L, Gurabi MA, Mandal A, Heitmann B. Towards Privacy-Preserving Sharing of Cyber Threat Intelligence for Effective Response and Recovery. ERCIM NEWS. 2021, 126:33.

[175] Imeri A, Rysavy O. Deep learning for predictive alerting and cyber-attack mitigation. In2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC) 2023 Mar 8 (pp. 0476-0481). IEEE.

[176] Mouratidis H, Islam S, Santos-Olmo A, Sanchez LE, Ismail UM. Modelling language for cyber security incident handling for critical infrastructures. Computers & Security. 2023 May 1, 128:103139.

[177] Al Sibahee MA, Ma J, Nyangaresi VO, Abduljabbar ZA. Efficient Extreme Gradient Boosting Based Algorithm for QoS Optimization in Inter-Radio Access Technology Handoffs. In2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) 2022 Jun 9 (pp. 1-6). IEEE.

[178] Körner MF, Sedlmeir J, Weibelzahl M, Fridgen G, Heine M, Neumann C. Systemic risks in electricity systems: A perspective on the potential of digital technologies. Energy Policy. 2022 May 1, 164:112901.

[179] Jghef YS, Zeebaree S. State of art survey for significant relations between cloud computing and distributed computing. International Journal of Science and Business. 2020, 4(12):53-61.

[180] Ray BK, Saha A, Khatua S, Roy S. Proactive fault-tolerance technique to enhance reliability of cloud service in cloud federation environment. IEEE Transactions on Cloud Computing. 2020 Jan 22, 10(2):957-71.

[181] Nyangaresi VO, El-Omari NK, Nyakina JN. Efficient Feature Selection and ML Algorithm for Accurate Diagnostics. Journal of Computer Science Research. 2022 Jan 25, 4(1):10-9.

[182] Zohuri B, Rahmani FM. Artificial intelligence driven resiliency with machine learning and deep learning components. Japan Journal of Research. 2023 Apr 17, 1(1).

[183] Maazouzi F, Zarzour H. AI-Driven Big Healthcare Analytics: Contributions and Challenges. InIntelligent Analytics With Advanced Multi-Industry Applications 2021 (pp. 172-184). IGI Global.

[184] Rahmani AM, Azhir E, Ali S, Mohammadi M, Ahmed OH, Ghafour MY, Ahmed SH, Hosseinzadeh M. Artificial intelligence approaches and mechanisms for big data analytics: a systematic study. PeerJ Computer Science. 2021 Apr 14, 7:e488.

[185] Davenport TH. From analytics to artificial intelligence. Journal of Business Analytics. 2018 Jul 3, 1(2):73-80.

[186] Paiola M, Schiavone F, Grandinetti R, Chen J. Digital servitization and sustainability through networking: Some evidences from IoT-based business models. Journal of Business Research. 2021 Aug 1, 132:507-16.

[187] Omollo VN, Musyoki S. Global Positioning System Based Routing Algorithm for Adaptive Delay Tolerant Mobile Adhoc Networks. International Journal of Computer and Communication System Engineering. 2015 May 11, 2(3): 399-406.

[188] Nakkiran P, Kaplun G, Bansal Y, Yang T, Barak B, Sutskever I. Deep double descent: Where bigger models and more data hurt. Journal of Statistical Mechanics: Theory and Experiment. 2021 Dec 29, 2021(12):124003.

[189] Georgios C, Evangelia F, Christos M, Maria N. Exploring cost-efficient bundling in a multi-cloud environment. Simulation Modelling Practice and Theory. 2021 Sep 1, 111:102338.

[190] HersterDudley MR. Building Resilience within DOD Microgrids by Considering Human Factors in Recovery Procedures (Doctoral dissertation, Monterey, CA, Naval Postgraduate School).

[191] Charles W, Marler N, Long L, Manion S. Blockchain compliance by design: Regulatory considerations for blockchain in clinical research. Frontiers in Blockchain. 2019 Nov 8, 2:18.

[192] Hoxey E. The challenge of keeping up with a rapidly changing regulatory landscape. Biomedical Instrumentation & Technology. 2017 May, 51(3):204-5.