ISSN 1816-6075 (Print), 1818-0523 (Online)
Journal of System and Management Sciences
Vol. 14 (2024) No. 1, pp. 1-14
DOI:10.33168/JSMS.2024.0101

A Novel Framework for Business Continuity Plan in Public Sector Organization

Ayu Artaparamita Religia, Ditdit Nugeraha Utama

Computer Science Department, BINUS Graduate Program - Master of Computer Science,
Bina Nusantara University, Jakarta 11480, Indonesia

ayu.religia@binus.ac.id; ditdit.utama@binus.edu

Abstract. Digital transformation in public sector organizations is closely linked to the utilization of information systems. However, a staggering 51% of organizations worldwide lack a Business Continuity Plan (BCP) to address disruptions to information systems. BCPs play a crucial role in ensuring the continuity of an organization's business processes during emergencies. While previous studies have proposed various BCP frameworks, none have specifically focused on the business processes of public sector organizations. Given each organization's unique strategies and business processes, it is essential to customize a BCP framework to meet the specific needs of public sector entities. This research introduces a new framework for developing BCP specifically designed for public sector organizations. This research combines two standard frameworks, ISO 22301:2019 and NIST SP 800-34 Rev.1. This approach results in a structured and comprehensive BCP framework for managing information systems in public sector organizations. This framework serves as a tool to assist public sector entities in effectively managing potential disruptions, minimizing downtime, and maintaining their business processes in the face of emergencies.

Keywords: Business Continuity, BCP, Public Sector, Information Systems

1. Introduction

The current digital transformation era is related to the utilization of information systems. Many organizations make digital changes to support their business process activities, not only in profit-oriented but also in public sector organizations. Digitalization simplifies and runs business processes in public sector organizations more effectively and efficiently (Bjerke-Busch & Aspelund, 2021). This digitalization makes information systems have a vital role in organizations. If things happen that are not desirable to the information systems, it can cause significant losses to the cessation of the organization's business processes (Moşteanu, 2020). Some potential disruptions for information systems are cybercrime, natural disasters, human error, device failure and procedural errors (Kassema, 2020). This disruption can impact public sector organizations' decision-making process and operational activities, affecting reputation and decreasing service user satisfaction (Bakar et al., 2019).

Therefore, organizations need a plan to anticipate things that could be more desirable for information systems. This plan is called a Business Continuity Plan (BCP) (Akbari & Gurning, 2020). BCP is a procedure to keep the organization's business functions running before, during, and after a disruption (Snedaker & Rima, 2014), BCP must ensure business processes can continue operating in an emergency (Yuliansyah & Soewito, 2020). However, many organizations, especially public sector organizations, must realize the importance of making a BCP (Fani & Subiadi, 2019). According to a survey conducted by Mercer in 2020, 51% of organizations worldwide do not have BCPs for emergencies (Baptista, 2020). This survey shows that BCP has not become an organizational priority. One reason is the limited knowledge of BCP development (Febria et al., 2018).

Various studies have been conducted to propose a BCP framework. According to research conducted by (Nnebe et al., 2018), BCP was built by presenting a new framework model. While on the other research conducted by (Pramudya W. & Fajar, 2019), built BCP using framework standards such as ISO 22301: 2012 and BCI GPG 2013 then implemented in profit-oriented organizations. Based on the results of previous studies, the BCP framework implemented for public sector organizations still needs to be improved. It is necessary to adjust the framework to manage information systems for public sector organizations' needs. Due to different organizational needs, each organization will have a different BCP. (Roy, 2022).

To address this gap, this research proposes a BCP framework and stages to support public sector organizations in enhancing their preparedness and maintaining the continuity of critical business processes even during information system disruptions. Using a different approach from previous research, the development of the framework and stages combine two reference standards, ISO 22301:2019 Business Continuity Management Systems Framework standard and the Contingency Planning Guide for Federal Information Systems, NIST SP 800-34 Rev.1 standard, which also describes the elements of BCP.

2. Literature Review

In this section, we will discuss explanations relevant to this research and previous research conducted related to BCP.

2.1. BCP

Business continuity is the organization's ability to continue the process during disruption. Business continuity can be influenced by several factors, such as data and application availability, network, and operating system reliability (Anir et al., 2019). Organizations need to strengthen their digital management systems by building a comprehensive security management system and increasing employee security awareness to deal with disruptions to information systems (Wang & Lee, 2023). In this condition, organizations need a plan to maintain the continuity of business processes. This plan is called a Business Continuity Plan (BCP) (Awasthi, 2021). BCP is a method or process prepared by the organizations to deal with things that are not desirable. BCP is built to protect assets, information, and

personnel during and after a disruption (Tiwary & Sandhane, 2022). Information asset protection is dependent on creating an information security plan and applying security controls as part of that plan (Abakar et al., 2022). Currently, not only essential, but now BCP has become a necessity, especially for public sector organizations where the primary business process services and carried out online through information systems (Bakar et al., 2019). The focus of the BCP plan should be on critical processes and interdependencies. Furthermore, BCP governance includes elements such as commitment, controls, management direction, clearly written roles and tasks, formal governance processes and ensuring that the BCP is continuously updated (Andi & Utama, 2023). To help organizations build a BCP, several standard framework models can be adopted. These framework standards can help organizations identify the potential impact of various disruptions on the organizations and can prioritize efforts to maintain business process continuity (Supriadi & Pheng, 2018).

2.2. ISO 22301:2019

ISO 22301:2019 is a standard that outlines the requirements for the implementation of a Business Continuity Management System (BCMS). This standard helps organizations to prepare for, prevent, respond to, and recover from incidents of disruption such as natural disasters, cyberattacks and other undesirable events. This standard provides a framework for organizations to identify disruptions, assess impact, develop strategies for mitigation and establish procedures to ensure business continuity in the event of a disruption. In implementation, ISO 22301: 2019 framework standard has 10 clauses, but for the needs of the BCMS aspect, the clauses used start from clause 4 to clause 10 and applies the Plan Do Check Act (PDCA) cycles (International Organization for Standardization, 2019).

2.3. NIST SP 800-34 Rev.1

NIST is the standard developed by the National Institute of Standards and Technology (NIST). This standard is prepared for federal organizations. NIST standards perform five security controls for organizations. These controls are identify, detect, protect, respond, and recover data and assets (Al-Matari et al., 2021). One of the standards is NIST SP 800-34 Rev.1. This standard provides framework guidance for developing and maintaining contingency plans for information systems (Prasetyo et al., 2019). The NIST SP 800-34 Rev.1 framework outlines the process of managing BCP and DRP based on organizational needs (Jorrigala, 2017). For the Contingency Plan development process, NIST SP 800-34 Rev.1 has seven stages (National Institute of Standards and Technology, 2010).

3. Related Works

Various studies have also been conducted to build BCP by using or modifying existing framework standards. One of them, the author (W & Fajar, 2019) built BCP using the ISO 22301: 2012 framework standard and implemented it in an IT solution company. The ISO clauses used in this research BCP framework are Clause 4 Context of Organization, clause 5 leadership, clause 6 planning and clause 7 Support. This study also conducted a risk assessment and identified potential threats that could impact business processes. As a result of this research, the BCP framework created can help organizations identify potential risks and develop effective strategies to mitigate them. However, the success of BCP also depends on testing and training to remain relevant and effective.

Another research conducted by (Febria et al., 2018) built BCP using the ISO 22301: 2012 and BCI GPG 2013 framework standards. This framework was then implemented in electronic banking services. The stages of BCP development are risk assessment, business impact analysis, BCP Strategy and Handling, and BCP stage. The results of this study show that the BCP that was built still had to be updated continuously because not all stages in the ISO 22301 and BCI GPG 2013 standards are used in BCP development. Research (Fani & Subriadi, 2019) the BCP framework was built using the ISO 22301: 2012 framework standard and COBIT 5 Domain: Manage Continuity. This framework examines four organizations. The BCP framework in this study has eight components and 38 processes. The result still needs further research on the effectiveness of this BCP framework, especially for public sector

organizations, because this BCP framework still needs to be implemented.

In research by (W & Fajar, 2019), (Febria et al., 2018) and (Fani & Subriadi, 2019), author build BCP by using existing framework standards. Meanwhile, there is research that proposes a new BCP framework model to answer organizational needs. Such as research conducted by (Nnebe et al., 2018) proposes a new BCP framework built with 4 stages 1. Prevention measurement, 2. Monitoring and incident detection, 3. reports and investigations, 4. implementation and testing. The framework is classified into 2 (two) perspectives, namely the incident discovery phase and the incident response phase. The results of this study emphasize the importance of involving all parts of the BCP development, from management to all staff, not just the IT department.

Meanwhile, the author (Soufi et al., 2018) proposed a new BCP framework with a quantitative model. The proposed framework consists of four stages: risk assessment, impact analysis, mitigation planning, and testing and maintenance. The risk assessment stage is carried out by identifying potential threats to the organizations and assessing the likelihood and impact of each threat. The business impact analysis stage is carried out by analyzing the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) of the business process. The mitigation planning stage is carried out by developing a series of actions to reduce the identified threats' impact; the last stage is testing and maintenance. At this stage, BCP is tested to ensure its effectiveness. This framework was applied to a manufacturing company then. Research by (Al Ali et al., 2020) propose a framework specifically for Internet of Things (IOT). The authors emphasize the importance of the security and privacy aspects of IoT systems. The proposed framework consists of risk assessment, business impact analysis, business continuity plan, incident response and recovery strategies, and regular testing and updating of the plan. This research conclude for effective framework is needed for proactive planning, effective incident response, and collaboration among stakeholders in ensuring the resilience of IoT systems.

As a conclusion from the literature review on previous studies, BCP is built according to the needs and conditions of the organization. There are no specific guidelines related to the standard framework or structure for public sector organizations in building BCP. Some studies only explain the BCP framework with some elements that must be included. The previous study found minimal literature available on the experiences of BCP within the public sector experience.

4. Research Methodology

This research follows a systematic methodology consisting of five stages to develop the BCP framework for public sector organizations. Fig. 1 illustrates the research stages, which are problem analysis, literature review, framework analysis and join, data collection and analysis, and the stages construction of BCP Development. The first stage, problem analysis, involves identifying the challenges faced by public sector organizations in managing information systems and the potential disruptions that may impact their business processes.

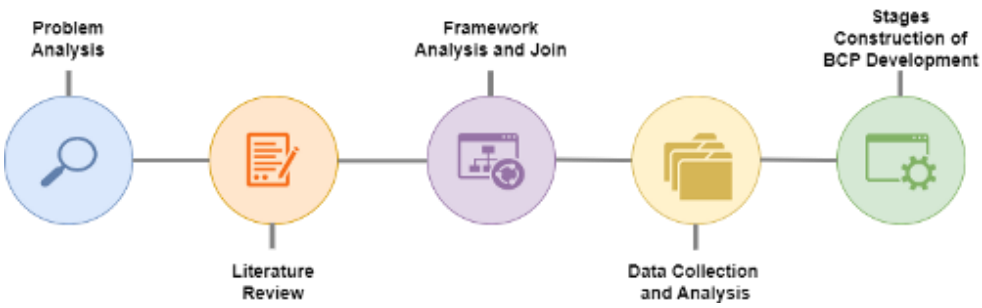

Fig. 1: Research Stage

After doing problem analysis, proceed with the literature review stage to study some theories, previous research, and existing framework concepts related to BCP. The framework analysis and join

stage is a critical phase in this research. Two reference framework standards are analyzed and union to create a comprehensive BCP framework that suits the needs of public sector organizations. This process involves analyzing the components of the standards and integrating them to form a cohesive framework. Data collection and analysis is the subsequent stage, carried out within a specific public sector organizational unit involved in infrastructure management. Various activities such as document collection, interviews with key personnel responsible for information systems, and observations are conducted. Additionally, organizational needs related to BCP are identified and documented at this stage.

The next stage is the construction stage of BCP development. After obtaining information and organizational needs, the next thing to do is to build the BCP stages to get a more structured and effective BCP. The method used at this stage is mapping organizational needs with the components of the new framework. The results of this mapping are the stages used for BCP development based on the needs of public sector organizations. After the BCP development stages are created, it is necessary to evaluate whether the BCP stages proposed in this research can meet the organization's needs. This assessment is an evaluation process. The evaluation was conducted by mapping the proposed BCP development stages into the PDCA cycle and using a questionnaire distributed to IT staff who manage information systems in public sector organizations. This evaluation assesses whether the proposed BCP stages adequately meet the organization's needs and identifies any necessary improvements or modifications.

4.1. Proposed Method

This research proposes a new BCP framework by combining two reference standards. The process of developing this framework involves three distinct steps. The first step involved identifying the two reference standards' functions, advantages, and disadvantages. This assessment provided a comprehensive understanding of the strengths and weaknesses of each standard and laid the foundation for their integration.

In the subsequent analysis step, the components of the two standards were thoroughly examined and compared. The purpose was to determine the compatibility and alignment between the components of the reference framework standards. This analysis aimed to identify areas of overlap, complementarity, and potential gaps that needed to be addressed in developing the new BCP framework. Finally, the join phase applies a union operation approach to smoothly merge the compatible components collected from the reference framework standards in the third stage. This thorough integration process enables the establishment of a single and cohesive BCP framework that integrates the most important and effective parts from both standards, allowing enterprises to manage disruptions successfully and assure the continuity of critical business processes. Fig. 2 shows the fundamental steps of the framework analysis and join stage.

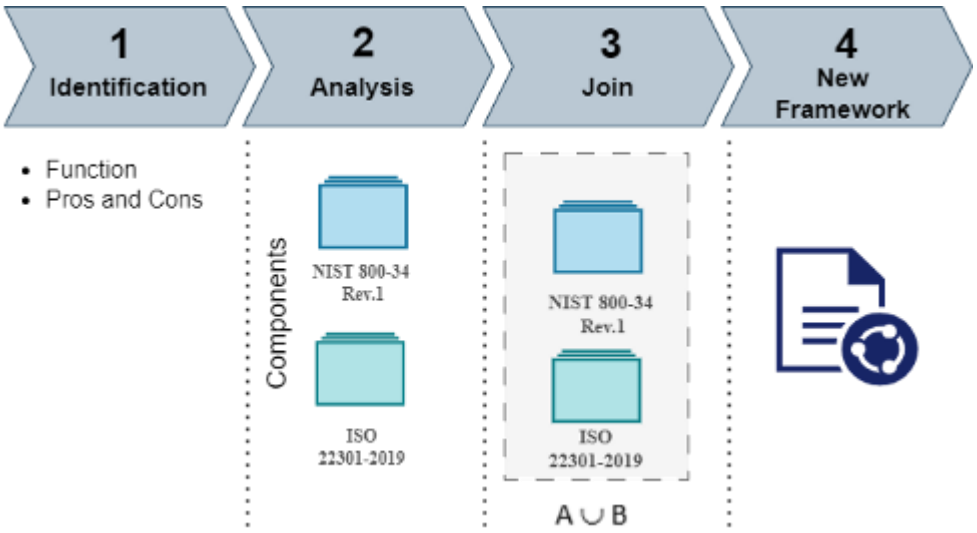

Fig. 2: Step of Framework Analysis and Join

5. Result and Discussion

From the analysis problem stage carried out that in public sector organizations when dealing with unwanted things that occur, such as disruption in information systems that support business processes, there is no segregation of duties, still limited knowledge related to security awareness among management and employees and a lack of documentation to handle the disturbances. Furthermore, a literature review was conducted to build a BCP framework in public sector organizations. Moreover, from the results of the literature review stage, two standards were used as references for this research: ISO 22301: 2019 standard for Business Continuity Management system and NIST SP 800-34 Rev.1 standard is a contingency plan guideline for federal information systems.

Table 1: Identification Reference Standards

	ISO 22301:2019	NIST SP 800-34 Rev.1
Functions	Continuity of business operation	Continuity of information systems
Pros	a. Have Comprehensive process. b. Can be applied to all parts of the organizations. c. ISO standards are well known.	a. More relevant to public sector organizations because the standard was built for federal information systems. b. The requirements are not complicated. c. Allowing organization to construct as needed
Cons	a. The standard complexity may be difficult to implement for some organizations. b. May requires a lot of resources to construct and maintain	a. Specific guideline, only for continuity of information system b. Not provide a comprehensive framework for business continuity

The first step in the framework analysis and join stage is identification. The literature review found that the two reference framework standards have some of the same processes for BCP development. So, in this step, a more profound identification is carried out regarding each framework standard's functions and advantages and disadvantages. Table 1 is the result of the identification step of the reference standard. From the results of this identification step, both standards have functions to build a BCP framework.

The advantages of the ISO 22301: 2019 standard include a comprehensive process that can be applied to all parts of the organizations because it uses the PDCA cycle. But the complexity of ISO 22301: 2019 can make this standard harder to implement for organizations just about to build a BCP. Meanwhile, the NIST 800-34 Rev.1 standard has a simpler process and is suitable for public sector information systems. The next step is analysis, this step is to ascertain what requirements are needed to build a BCP. This step is carried out by describing the components of the two standards as written in Table 2.

From the table, it is obtained that ISO 22301: 2019 has 10 clauses and 25 required processes, while NIST SP 800-34 Rev.1 contains 7 steps and 31 processes followed starting from policy, conduct Business Impact Analysis (BIA), Identify preventive controls, create contingency strategies, develop contingency plans, plan testing, training, and exercises, to plan maintenance. After the analysis, the next step is the join step. The activity carried out in this step is the union of the analyzed components of the two standards. The union results of all components of the two standards are in Table 3. There are a total of 16 components in the column. The components in the union column are the new BCP framework used to build BCP for information system management in public sector organizations. Then given the combined component merge code using the UN code.

Table 2: Reference Standards Component

Clause	ISO 22301:2019	NIST 800-34 Rev.1
1	Scope	Policy
2	Normative references	Business Impact Analysis (BIA)
3	Terms and definitions	Preventive Controls
4	Context of the Organization	Contingency Strategies
5	Leadership	Contingency Plan
6	Planning	Testing, Training and Exercises (TT & E)
7	Support	Maintenance
8	Operation	
9	Performance evaluation	
10	Improvement	

The components of the new framework are Scope (UN1) which describes the areas and aspects to be covered by the BCP. Normative references (UN2) provide a list of applicable references that serves as a guideline. Meanwhile, Terms and definitions (UN3) provide a list of terms and definitions that will be used consistently. The context of the organization (UN4) component focuses on identifying issues that can affect the organization. Leadership (UN5) highlights the importance of top-level management commitment to the BCP, a critical factor in successful implementation. Planning (UN6) involves the development of a BCP that includes business impact analysis, identification of business continuity strategies, and comprehensive planning. Supporting information (UN7) provides resources, training, awareness, communication, and documentation required in BCP implementation. Operation (UN8) covers BCP implementation steps, such as risk assessment, business continuity strategy implementation, and piloting and testing. Develop Business Continuity Plan (UN9) focuses specifically on developing procedures that address potential risks and disruptions. While Creating Contingency Strategies (UN10) involves the development of alternative plans or actions to mitigate risks. The Identify Preventive Controls (UN11) component covers identifying potential threats, vulnerabilities, and preventive

controls required to mitigate risks. Performance evaluation (UN12) is for monitoring and evaluating BCP performance regularly, while Training requirements (UN13) focus on the effectiveness and sustainability of training required by relevant personnel. Plan Testing, Training, and Exercises (UN14) are for carrying out planned testing, training, and exercises to ensure BCP readiness. Plan Maintenance (UN15) emphasizes the importance of maintaining the sustainability and effectiveness of the BCP by making updates and adjustments as needed by the organizations. Finally, Improvement (UN16) emphasizes the importance of continuous improvements to ensure BCP effectiveness and readiness. With these 16 components, the new BCP Framework becomes more comprehensive and effective for the continuity of business processes of public sector organizations.

Table 3: Union BCP Framework

Union Component	Union Code	Explanation
Scope	UN1	Outlines the scope of the framework
Normative references	UN2	Lists the normative references that are applicable
Terms and definitions	UN3	List of terms and definitions
Context of the Organization	UN4	Determine the issues that can impact organization
Leadership	UN5	Top management commitment
Planning	UN6	BCP plan, developing a business impact analysis, identifying business continuity strategies
Supporting Information	UN7	Providing supporting information such as resources, training, awareness, communication, and documentation
Operation	UN8	Implementing risk assessment and business continuity strategies
Develop Business Continuity Plan	UN9	Involve the development of procedures and plans that address specific risks and potential disruptions
Create Contingency Strategies	UN10	Developing alternative plans or actions to mitigate risks.
Identify Preventive Controls	UN11	Identify potential threats, vulnerabilities, and preventive controls
Performance evaluation	UN12	Monitoring and evaluating performance
Plan Testing, Training and Exercises	UN13	Testing, training, and exercising the business continuity plan
Plan Maintenance	UN14	Keeping the business continuity plan current in terms of effectiveness and applicability
Training requirements	UN15	Effectiveness and sustainability
Improvement	UN16	Continually improving

After the new framework was built, the current needs and conditions of one of the public sector organizations' cases were explored through the data collection and analysis stage. The information obtained was related to business processes, organizational resources, and the organization's need for BCP. This organizational unit has 64 information systems used to support 19 business processes. Organizational needs related to BCP development are following the duties and functions of the organization's information systems management, easy to implement, contains helpdesk information, can mitigate risks, and reduce impacts when disruptions occur, can provide recommendations for priority recovery strategies, dynamic and follow organizational and technological changes.

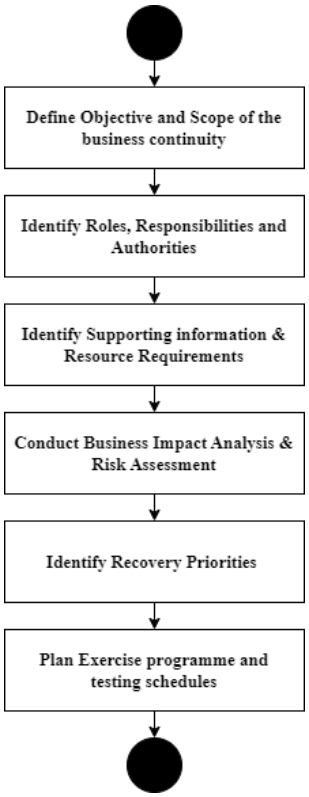

Fig.3: Stages of BCP Development

The results of this stage are then used as basic information to determine the stages of BCP development. Furthermore, the stages construction of BCP development is carried out by mapping the results of exploring organizational needs related to BCP for information system management with the components of the new framework. From the mapping, it is obtained that the stages of BCP development for information system management of public sector organizations. The stages of the proposed BCP development are shown in Figure 3. The stages consist of 6 components from 16 components of the new framework.

After the BCP development stages are made, an evaluation is conducted to assess whether the proposed BCP development stages meet the organization's needs. The evaluation is carried out by mapping the stages into the PDCA cycle. This is done because PDCA is a standard methodology used to support continuous process improvement (Patel & Deshpande, 2017). Results from mapping the BCP development stages into the PDCA cycle, each component of the proposed BCP development stages supports the cycle phase of PDCA shown in Figure 4. The PLAN phase is the stage of defining and scoping the BCP, identifying roles and responsibilities, and identifying supporting information and resource requirements, in the DO phase is conducting business impact analysis, conducting risk assessment, and identify priority recovery strategies, then in the CHECK phase designing a testing schedule, and in the ACT, phase conducting an exercise program.

Fig. 4: Mapping the stages into PDCA Cycles.

Besides mapping the stages into the PDCA cycle, the evaluation was also carried out through a questionnaire given to the IT staff of the organization using a summated rating scale or Likert scale. The assessment through this questionnaire was carried out by asking 10 questions related to the 6 stages proposed for the development of BCP for public sector organizations. Respondents were given 5 answer scales: strongly agree, agree, neutral, disagree, and strongly disagree. 48 respondents' responses were collected by filling out the questionnaire.

Table 4: Questionnaire Result for BCP Stages

	SS	S	N	TS	STS	Score Question	Avg
Q1	24	21	2	0	1	211	4.40
Q2	19	23	5	0	1	203	4.23
Q3	20	23	4	0	1	205	4.27
Q4	16	22	9	0	1	196	4.08
Q5	19	21	6	0	2	199	4.15
Q6	18	25	4	0	1	203	4.23
Q7	28	16	3	0	1	214	4.46
Q8	24	18	5	0	1	208	4.33
Q9	22	22	3	0	1	208	4.33
Q10	26	14	7	0	1	208	4.33
						2055	42.81

$$TS = \frac{\sum Avg}{\sum Q} \quad (1)$$

Table 4 shows the questionnaire results provide insights into evaluating the proposed BCP stages for public sector organizations. The calculation of the questionnaire results reveals that the average scores for each question range from 4.08 to 4.46. Question 7 obtained the highest average score of 4.46, indicating a strong agreement among respondents. On the other hand, question 4 received the lowest average score of 4.08, suggesting a slightly lower level of agreement than the other questions.

Calculating the total average score using equation 1, which considers $\sum Avg$ is the average total score and $\sum Q$ is the total number of questions, determines the overall score to be 4.28. This score reflects the overall evaluation of the respondents regarding the proposed BCP stages. Furthermore, the percentage of the questionnaire results is calculated using equation 2, where TS is the total score from the calculation of equation 1 divided by NS the Likert scale point value (5 in this case). The calculation yields a total percentage of 85.63%. This indicates that 85.63% of the respondents agreed with the proposed BCP stages, implying that the stages are aligned with the needs of public sector organizations in developing BCP.

$$TP = \frac{TS}{NS}100 \quad (2)$$

These findings suggest that the proposed BCP stages have received positive feedback from the IT staff members who participated in the questionnaire evaluation. The high agreement percentage demonstrates that the stages are perceived to be suitable for public sector organizations and can effectively contribute to the development of BCP in their information systems management. It is important to note that the questionnaire evaluation is based on the perspectives of the IT staff members of a specific organization. Therefore, the results may not be generalized to all public-sector organizations. However, the positive response and high agreement percentage indicate the potential practical value and relevance of the proposed BCP stages in the context of the studied organization.

6. Conclusions and Further Works

As the reliance on information systems grows in public sector organizations to support their business processes, developing a robust Business Continuity Plan (BCP) becomes crucial to anticipate and mitigate potential disruptions. A key component of BCP development is the framework, which should be tailored to public sector organizations' specific needs and challenges. This research addresses this need by proposing a BCP framework that combines the ISO 22301:2019 and NIST SP 800-34 Rev.1 framework standards.

The resulting framework is structured, comprehensive, and aligned with international best practices. By integrating the specific requirements of managing information systems in public sector organizations, the framework provides a systematic approach to developing BCPs that ensures the continuity of essential business processes. Public sector organizations can utilize this framework to manage potential disruptions to their information systems better, enhance their resilience, and maintain the smooth operation of critical business functions. Organizations can benefit from a well-designed framework that guides their BCP development efforts, ensuring a comprehensive and systematic approach to managing information system risks. Alignment with internationally recognized standards enhances the credibility and reliability of the framework, enabling organizations to adhere to best practices and benchmark their BCPs against industry standards. The adaptability of the framework allows it to be tailored to the unique needs and contexts of different public sector organizations, regardless of their size or nature. However, it is important to acknowledge the limitations of this research. The findings are based on a specific organization or a limited number of organizations within the public sector, which may limit the generalizability of the results. Additionally, the evaluation of the

framework's effectiveness primarily relied on feedback from IT staff members through a questionnaire, and further evaluation involving stakeholders from different organizational levels is warranted. External factors such as budget constraints and organizational culture may also impact the framework's implementation and effectiveness.

Suggestions for future studies should consider implementing the framework in various types of organizations. This will help determine its effectiveness, adaptability, and scalability in different contexts, ensuring its relevance and applicability across diverse public sector settings. Further research and implementation of the framework in different organizational contexts will contribute to its ongoing refinement and validation, ultimately benefiting the resilience of public sector organizations in the face of information system uncertainties.

References

Abakar, S. M., Musa, A. I., & Younis, A. M. (2022). A Study on Cybersecurity Awareness among Sudanese Companies during Covid-19. *Journal of System and Management Sciences, 12*(3), 200-215. doi:10.33168/JSMS.2022.0311

Akbari, D. R., & Gurning, R. O. (2020). Development of Risk Based Business Continuity Plan Using House of Risk Method on Container Terminal. *IOP Conference Series: Earth and Environmental Science, 2nd Maritime Safety International Conference (MASTIC). 557.* Surabaya: IOP Publishing Ltd. doi:10.1088/1755-1315/557/1/012024

Al Ali, J., Nasir, Q., & Dweiri, F. T. (2020). Business continuity framework for Internet of Things (IoT) Services. *International Journal of System Assurance Engineering and Management, 11*, 1380-1394. doi:0.1007/s13198-020-01005-7

Al-Matari, O. M., Helal, I. M., Mazen, S. A., & Elhennawy, S. (2021). Adopting security maturity model to the organizations' capability model. *Egyptian Informatics Journal, 22*(2), 193-199. doi:10.1016/j.eij.2020.08.001

Andi, R., & Utama, D. N. (2023). Business Continuity Management Framework In Electronic System Provider (ESP) Startup Company. *Journal of System and Management Sciences, 13*(1), 322-343. doi:10.33168/JSMS.2023.0118

Anir, H., Fredj, M., & Kassou, M. (2019). Towards An Approach For Integrating Business Continuity Management Into Enterprise Architecture. *International Journal of Computer Science & Information Technology (IJCSIT), 11*(2), 1-16. doi:10.5121/ijcsit.2019.11201

Awasthi, A. (2021). IT Infrastructure - Business Continuity Plan Implementation and Maintenance. *Journal of Information Technology & Software Engineering, 11*(2), 1-9. Retrieved from https://www.longdom.org/abstract/it-infrastructure-engineering-restoration-hardware-64611.html

Bakar, Z. A., Yaacob, N. A., Udin, Z. M., Hanaysha, J. R., & Loon, L. K. (2019). Business Continuity Management Implementation in the Malaysian Public Sector. *International Journal of Business and Technology Management, 1*(1), 18-27. Retrieved from http://myjms.mohe.gov.my/index.php/ijbtm

Baptista, A. (2020). *51% of companies have no business continuity plan to combat coronavirus outbreak: Mercer study finds*. (mercer) Retrieved 2 5, 2023, from https://www.mercer.com/content/dam/mercer/attachments/global/gl-2020-mercer-covid-19-global-survey-coronavirus-impact-to-global-market.pdf

Bjerke-Busch, L. S., & Aspelund, A. (2021). Identifying Barriers for Digital Transformation in the Public Sector. *Digitalization. Management for Professionals.*, 277-290. doi:10.1007/978-3-030-69380-0_15

Fani, S. V., & Subiadi, A. P. (2019). Trend of Business Continuity Plan: A Systematic Literature Review. *Proceedings of the Proceedings of the 1st International Conference on Business, Law And Pedagogy.* Sidoarjo: EAI. doi:10.4108/eai.13-2-2019.2286164

Fani, S. V., & Subriadi, A. P. (2019). Business Continuity Plan: Examining of Multi-Usable Framework. *The Fifth Information Systems International Conference, 23-24 July 2019, Surabaya, Indonesia. 161*, pp. 275-282. Surabaya: Procedia Computer Science. doi:10.1016/j.procs.2019.11.124

Febria, D. Z., Januanto, A., & Suroso, J. S. (2018). Business Continuity Plan on Electronic Banking Services (At Unit E. Channel Operation Bank XYZ) Using ISO 22301-2012 and BCI 2013. *Journal of Business Continuity & Emergency Planning*, 1-6.

International Organization for Standardization. (2019). *ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements.* International Organization for Standardization.

Jorrigala, V. (2017). Business Continuity and Disaster Recovery Plan for Information Security. *Culminating Projects in Information Assurance, 44*. Retrieved from https://repository.stcloudstate.edu/msia_etds/44

Kassema, J. J. (2020). Information Technology (IT) Contingency Plan as Part of the Business Continuity Plan: Case of IT Services Delivery Industry. *International Journal of Information Systems & Management Science*, *12*(2). doi:/10.2139/ssrn.3496143

Moşteanu, D. R. (2020). Management of Disaster and Business Continuity in a Digital World. *International Journal of Management, 11*(4), 169-177. doi:10.34218/IJM.11.4.2020.018

National Institute of Standards and Technology. (2010). *Contingency Planning Guide for Federal Information Systems.* National Institute of Standards and Technology.

Nnebe, S. E., Iyafokhai, I. U., & Sadiq, M. N. (2018). A Framework for Optimizing the Computer Security Incident Business Continuity Plan. *International journal of engineering research and technology*, *7*(11), 98-103.

Patel, P. M., & Deshpande, V. A. (2017). Application Of Plan-Do-Check-Act Cycle For Quality And Productivity Improvement - A Review. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, 197-201. doi:/10.22214/ijraset.2017.4181

Pramudya W., G., & Fajar, A. N. (2019). Business Continuity Plan Using ISO 22301:2012 in IT Solution Company (PT.ABC). *International Journal of Mechanical Engineering and Technology (IJMET), 10*(2), 865-872. Retrieved from https://iaeme.com/Home/issue/IJMET?Volume=10&Issue=2

Prasetyo, H. N., Supriatna, N., Raharjo, A. P., & Wikusna, W. (2019). Information Technology Disaster Recovery Plan (IT-DRP) Model-Based on NIST Framework in Indonesia. *International Journal of Applied Information Technology*, *03*(01), 34-45. doi:10.25124/ijait.v3i01.2317

Roy, A. (2022). Analysis of Business Continuity Plan in Banking Sector. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, 982-987. doi:10.22214/ijraset.2022.46326

Snedaker, S., & Rima, C. (2014). *Business Continuity and Disaster Recovery Planning for IT Professionals 2nd Edition.* Syngress.

Soufi, H. R., Torabi, S. A., & Sahebjamnia, N. (2018). Developing a novel quantitative framework for business continuity planning. *International Journal of Production Research*, 779-800. doi:10.1080/00207543.2018.1483586

Supriadi, L. S., & Pheng, l. S. (2018). Business Continuity Management (BCM). In L. S. Supriadi, & l. S. Pheng, *Business Continuity Management in Construction* (pp. 41-73). Springer Nature. doi:10.1007/978-981-10-5487-7_3

Tiwary, R. K., & Sandhane, R. (2022). Designing Business Continuity Plan for It Organizations: A Systematic Literature Review. *Cardiometry, 24*, 849-858. doi:10.18137/cardiometry.2022.24.849858

Wang, Y., & Lee, E. L. (2023). Realizing Excellence in Enterprise Management through Digital Innovation. *Journal of Logistics, Informatics and Service Science, 10*(2), 197-211. doi:10.33168/JLISS.2023.0214

Yuliansyah, E., & Soewito, B. (2020). Asynchronous Multi-Site Method Design Disaster Recovery Center on the Business Process Automative Manufacturing (Case Study : PT XYZ). *Journal of Theoretical and Applied Information Technology, 98*(15), 3060-3079. Retrieved from https://www.jatit.org/volumes/Vol98No15/14Vol98No15.pdf