Information Security and Computer Fraud, 2024, Vol. 8, No. 1, 1-6
Available online at http://pubs.sciepub.com/iscf/8/1/1
Published by Science and Education Publishing
DOI:10.12691/iscf-8-1-1

Recommending Solutions for Contingencies Including Business Impact Analysis, Continuity, and Disaster Recovery

Cheryl Ann Alexander[1,*], Lidong Wang[2]

[1]Institute for IT Innovation and Smart Health, Mississippi, USA
[2]Institute for Systems Engineering Research, Mississippi State University, Mississippi, USA
*Corresponding author: cheryl.alexander@techhealthsolutions.org

Received May 10, 2024; Revised June 13, 2024; Accepted June 20, 2024

Abstract A business continuity plan (BCP) helps an organization mitigate cyberattacks, build resilience, and survive disasters. Unfortunately, many organizations' BCPs are too general and static (without enough consideration for condition changes) and do not work well when a disaster occurs, resulting in a loss of resources. It is necessary to enhance the adaptability and flexibility of a BCP so that the BCP is vigorous and adapts to changing conditions rapidly and easily. Business impact analysis (BIA) is a core component of a BCP. It is an effective approach to evaluating the potential effects of disturbances on critical business goals and procedures. BIA must consider any potential for change. An organization must also adapt or advance its BIA to guard against further cyber-attacks. This paper introduces BCP and BIA; deals with the BIA, continuity, and disaster recovery in healthcare systems; and presents a BIA case study of a medical center.

Keywords: *cybersecurity, business continuity plan, business impact analysis, disaster recovery, healthcare*

Cite This Article: Cheryl Ann Alexander, and Lidong Wang, "Recommending Solutions for Contingencies Including Business Impact Analysis, Continuity, and Disaster Recovery." *Information Security and Computer Fraud*, vol. 8, no. 1 (2024): 1-6. doi: 10.12691/iscf-8-1-1.

1. Introduction

A BCP is a document created by an organization that outlines the specific tasks and steps the organization needs to perform during and after a service disruption [1]. One of the primary opportunities to enhance the adaptability of a BCP is to analyze organizational risk and readiness now and under future conditions. BIA, a core component of a BCP, is generally static, based upon an organization's priorities and operating environment. BIA must consider the potential for changes so that a BCP is more robust and adaptive to changing conditions. It is important to identify key individuals with skills or knowledge within the organization, guarantee key knowledge is accessible, and offer effective cross-training that provides backup resources for key roles, hence improving internal resources — a key indicator of organizational resilience [2].

A documentary on Health Industry Cybersecurity Practices: Mitigating Threat and Protecting Patients covers five major threats identified in healthcare. They are 1) email phishing; 2) ransomware; 3) theft or loss of data or equipment; 4) internal, intentional, or accidental data loss; and 5) attacks against connected medical devices (possibly affecting patients' safety) [3]. Formulation and execution of a strong postattack BCP and/or contingency plans (CPs) is necessary to minimize disruption to patient care. The significance of cyberattack preparedness and CPs is not treated seriously in radiation oncology in hospitals. Both the preparedness and the awareness of smaller hospitals are not as good as those of larger hospitals. Education efforts in parallel with the development of suitable programs are needed to thwart pervasive and complex threats due to cyberattacks [4].

A security-first approach is necessary when discussing health BCPs. This includes fewer Ransomware risks and likely infections, a reduction in the security team's stress when an event does occur, and the health facility will experience more trust from partners and third-party allies. Cybersecurity is a team effort and requires the staff to be well trained. This paper deals with contingencies including BIA, continuity, and disaster recovery. The following is the arrangement of the rest of the paper: Section 2 introduces the BCP; Section 3 describes the BIA; Section 4 deals with the BIA, continuity, and disaster recovery in healthcare systems; Section 5 is a case study that presents the BIA in a Medical Center; Section 6 is the conclusion.

2. The Business Continuity Plan

The BCP plan is a set of procedures for maintaining business functions or swiftly getting them back up and running in case of some sort of major disruption such as

cyberattacks or a pandemic. The core components of an effective BCP include 1) a BIA, a critical first step — a process of finding significant business areas within an enterprise and their crucial functions to develop a plan; 2) calculating or estimating potential losses (generally classified into regulatory, financial, reputational, or legal losses) and attempting to know what impacts the losses have on the enterprise over various time lengths; 3) continuity procedures, focusing on CPs for processes and people in case of various interruptions [5]. Table 1 illustrates the contingency planning process [1]. Many enterprises have a high-level or very general BCP without specific actions to take in case of a disaster. This is because the enterprises have never tested their BCPs while testing is the only approach to measuring the effectiveness of the BCP. There are tools available to help develop BCPs. Some tools are free, e.g., online checklists and templates while others are not free of charge [5].

Table 1. The contingency planning process

Steps	Details
Develop contingency planning policies	Find regulatory or statutory requirements Prepare IT contingency planning policy statements Reflect FIPS 199 Publish policies
Conduct the BIA	Decide recovery criticality and business processes Find outage impacts & estimated downtime Determine resource requirement Decide recovery priority for a system
Find preventive controls	Find controls Execute controls Maintain controls
Develop contingency strategies	Backup and recovery Consider FIPS 199 Decide responsibilities and roles Address an alternate site Make equipment & cost considerations Integrate into a system architecture
Develop a contingency plan	Document the recovery strategy
Plan testing, training, and exercises (TT&E)	Plan testing Train personnel Plan exercises Perform TT&E activities
Plan maintenance	Review & update the plan Coordinate with internal or external organizations Control distribution Document change

FIPS: Federal Information Processing Standard

Traditional approaches to BC planning need to evolve to improve organizational resilience. It is crucial to guarantee a balance between detailed planning and flexibility as well as adaptability. This can be accomplished through 1) creating a closer link between BC and strategic management; 2) embedding a resilience culture throughout the organization; 3) decentralizing BC planning and enabling teams or departments to design and own their plans; 4) making planning principles-based; and 5) exercising more frequently. Planning should be based on the principle as well as outcome rather than the process, and how it must be integrated within broader risk management and strategy functions to be inclusive of everyone. A cycle of six BC management processes has been set out: 1) policy and program management, 2) analysis, 3) design, 4) implementation, 5) validation, and 6) embedding [2].

A disaster can be a loss of information, access, and personnel. The goal of the BC and disaster response planning process is to sort out various issues and priorities to develop a cost-effective plan. Both disaster recovery and BC require a high level of cooperation and coordination. Putting a team together and training it in advance will make all the difference in getting back to "business as usual." The process itself can be summarized in the following steps: 1) provide the management guideline; 2) detect serious risks; 3 prioritize operations to be maintained and how to maintain them; 4) assign the team; 5) take a complete inventory; 6) know where to get help; 7) document the plan; 8) review the plan with the entire staff, test the plan, and train the staff. A disaster preparedness plan should have contingencies for [6]:

- Generators for electricity and heat.
- Wi-Fi or other means to access the Internet.
- Alternate offsite practices to address emergency patient needs.
- An emergency gas supply for automobiles.
- A fireproof safe for cash and receipts.

Before establishing a plan to mitigate cybersecurity attacks, it is important to understand the change in the landscape that organizations have experienced regarding Disaster Recovery and Business Continuity (DRBC). A traditional DRBC plan includes two phases: 1) disaster recovery: which can include server and network restoration, copying backup data, and provisioning backup systems; 2) BC: the business operations side of DRBC can include staff replacement, service availability issues, BIA, and change management [3].

Table 2. Resilience indicators categorized by their planned and adaptive capabilities

Planned Capabilities	Adaptive Capabilities
Unity of purpose Planning strategies Proactive posture Stress testing plans Effective partnerships	Situational awareness Leveraging knowledge Staff engagement Innovation and creativity Leadership Decision making Internal resources Breaking silos

Table 3. IRBC controls recommendation

IRBC Elements	Assets	Controls
Technologies	OS, router, firewall	Log audit, hardening
	Sign Box	Patching, filtering, multi-factor authentication
	E-Sign APIs	App layer filtering
Processes	Data center service	Penetration testing
	E-Sign	Audit log
Facilities	Patch Panel	Fire suppression
	Access points	Log audit, hardening
	Server, Computers, UPS	Fault-tolerant systems
Knowledge and skills	Users	Security training
	Personnel	Gap analysis
Data	Procurement data	Periodic backup
	Employee data	Encryption/tokenization
Suppliers	Maintenance	Service level agreements
	Procurement	Assessment

Resilience is the ability to survive a crisis and thrive in a world of uncertainty. A resilience model with 13 indicators of an organization's ability to survive a crisis and thrive in a world of uncertainty is shown in Table 2 [7,8]. A possible resilience improvement for BC design is adding triggers in a BC plan. It is significant to design a BC system that enables sense changes as early as possible [2]. Security controls for the mitigation of risks are important, and the controls rely on information communication technology (ICT) greatly. The recommendation of ICT Readiness for Business Continuity (IRBC) is listed in Table 3 [9].

3. Business Impact Analysis

BIA is a main component of risk management and BC planning. It is a process of evaluating the impact over time of a disruption on the organization's products, people, services, and to its customers. To stay competitive, an organization must examine and adapt BIA when the circumstance changes, whether internally or externally. By considering organizational culture and standards, external and internal evaluation requirements, and standardized analysis, the organization will create a BIA that reflects its environment and still provides scope for improvement. Simply put, the successful development, implementation, and completion of the BIA depend on the alignment of its standards with the BC program, the organizational culture, audit requirements, and impact measures. Awareness of the maximum tolerable period of disruption (MTPD) is important when ranking recovery priorities to recover critical and non-critical business functions, and a condition of the ISO 22301, Security and Resilience Business Continuity Management System Requirements [10]. Three steps are involved in accomplishing the BIA [1]:

- Decide mission/business processes and recovery criticality, including the processes, the impacts of a system disruption to the processes, and estimated downtime.
- Identify resource requirements to continue mission/ business processes and related interdependencies. Examples of resources include personnel, facilities, equipment, system components, software, data files, and vital records.
- Decide recovery priorities for system resources. Priority levels can be created for sequencing recovery resources and activities.

BIA has been employed to evaluate impacts on an enterprise when an interruption occurs in supplying services or products that are vital to its operations. It is mainly utilized as an input to risk analysis and BC management (BCM). BIA largely involves the expert decision of the minimum level of resources that are needed to restore essential activities within a specified time and level. It is needed to decide the MTPD, the medium impact period of disruption (MIPD), and the maximum tolerable data loss (MTDL) parameters, which decide how data sets must be handled in case of recovery and backup. The parameters mainly decide the BCM for information assets, as well as the recovery time objective (RTO) and the recovery point objective (RPO) parameters. RPO is the time from which the last backup was taken. RTO is the time needed to make the application available again. In deciding the parameters, baseline conditions were assumed, where RPO <= MTDL, RTO <= MIPD, and RTO <= MTPD [11].

BIA is an effective approach to evaluating the potential effects of disturbances on critical business goals and procedures. Significant advancements have been made in integrating risk management and BIA. The integration has been suggested in a method for BCM. A framework was proposed based on a hybrid fuzzy BWM-TOPSIS method to identify crucial physical assets. Fuzzy BWM-TOPSIS is a decision-making approach to combining Fuzzy BWM (the best-worst method) and TOPSIS (a technique for order preference by similarity to the ideal solution). It facilitates deciding the relative importance of criteria and the performance of alternatives according to the decision-makers perceptions and then ranking the alternatives based on their proximity to the ideal solution. The framework incorporates BIA to decide essential products, a physical asset risk assessment matrix to evaluate critical assets based on the likelihood and impact, and a mathematical model for the estimation of asset continuity parameters. By adopting this framework, an enterprise can efficiently manage physical assets, prioritize continuity plans, and deal with resource constraints and uncertainties [12].

As governments progressively rely on electronic systems to provide basic services, the requirement for ICT BCPs becomes paramount. The risk decision involves evaluating the risk level for assets based on the mix of likelihood and impact levels (L: low; M: medium; H: high; H+: very high). Table 4 shows cyber risk assessment with the risk levels of various assets [9].

Table 4. Cyber risks assessment

Categories	Assets	Consequences	Likelihood	Impacts
Hardware	Firewall W	Downtime	H	H
	Router X	Router hack	H	H
	Access points	Wi-Fi hack	H	H
	Server Z	Downtime	H	H
	Computers C1-C23	Damage, error	M	H
	Uninterrupti-ble power supply (UPS)	Fire	H	H+
Software	OS, Antivirus	Malware	M	H
	Sign Box	Malware	M	M
	E-Sign APIs	Downtime	M	H
Human resource	Personnel	Insider threat	H	H
	Personnel	Human error	H	H
Information	Procurement data	Data loss	H	H
	Employee data	Data theft	H	H
	Configuration data	Data loss	H	H

4. Business Impact Analysis, Continuity, and Disaster Recovery in Healthcare Systems

Hospital information systems (HISs) encounter various risks (possible harm to human health). Risk assessment is a significant step of risk management. Evaluation of possible risks/threats in an HIS and presenting appropriate risk treatment plans (RTPs) enable system developers and managers to take proper actions when encountering various risks. RTPs usually include mitigation plans and BCPs within the context of BCM. To respond to the risks, a practical fuzzy risk evaluation framework was built under BCM concepts. The framework benefits from a fuzzy inference system and a fuzzy multi-criteria decision-making method to analyze and quantify the uncertain information collected from experts. The following steps help make BCPs [13]:

- Discover the risks with low probability but high impacts (significance difference)
- Find related key HIS services
- Identify the HIS risk appetite
- Conduct BIA to decide BIA parameters such as the MTPD and the minimum BC objective
- Present appropriate BCP strategy for the key service
- Execute resource planning to accomplish the defined strategy based on the risk priority
- Review and practice the developed BCPs

The following integral and universal components were suggested to be considered for inclusion in hospital BCPs: 1) alternative methods and resources, 2) the priority of operations, and 3) resource management. Even if the types and extent of disasters vary, the development of BCPs and BCM strategies that use the above integral components help a hospital to build resilience and survive disasters in the future [14].

To protect patient information, the HIPAA security rules require practices to have CPs in case of a fire, natural disaster, vandalism, or system failure. The plan should include policies and procedures for a response to an emergency that destroys health IT systems, and it needs to support the practice in adhering to significant aspects of the HIPAA security rules, such as the suitable approach to the disposal of a destroyed server that stores protected health information. Electronic health records should be backed up twice daily. Two components of the CPs that address the recovery should already be part of IT policies and procedures: 1) the plan of data backup: establishing procedures for the regular storage and update of personal health information (PHI); 2) the plan of data recovery: dealing with procedures of restoring data [6].

A conceptual and comprehensive framework was developed for a hospital. The framework components are composed of 1) in-hospital BCPs (offering basic service and getting help from unaffected areas); 2) hospital management for disaster risk reduction (DRR) outside a hospital (fostering community management and infrastructure resilience; reinforcing healthcare coalitions). The framework of the initial model with three indicators for disaster-resilience of hospitals is shown in Table 5 [15].

Hospital preparedness in response to mass casualty incidents (MCIs) and disasters includes the prior development and realization of systems, programs, and actions. Evaluating readiness for incidents or disasters, along with response efficiency, helps discover and handle potential gaps and weaknesses in hospital management during a disaster. Table 6 shows a hospital preparedness checklist with categories and subcategories [16].

Table 5. Indicators to evaluate disaster-resilient hospitals

Indicators	Description
Leadership and in-hospital BCP	Defining the region of the impact of a hospital Hospital structure for disaster preparedness Guaranteeing the effectiveness of the BCP
Hospital management for DRR outside a hospital	Enhancing community independence during a disaster: *Organizational structure of the hospital for the improvement* *Community engagement Improvement for disaster preparedness* *Supply chain improvement for the preparedness during daily-based operations*
	Empowering the healthcare coalition for disaster preparedness: *Hospital structure for the healthcare coalition in the region* *Disaster preparedness promotion of the medical community in the region* *Disaster preparedness promotion of service providers in a long-term care system*

Table 6. Readiness of incidents or disasters in hospitals

Categories	Subcategories
Medical products and technology	Personnel protective equipment and other equipment Medical stockpile Logistics and management Supportive functions
Hospital information systems	Infrastructure Patients/victims information Alert systems
Health workforce	In-hospital teams Hospital staff Assisting emergency medical teams
Participation	Coordination with other relevant organizations/agencies
Service delivery	Patients/victims care/management Hospital MCI plans/protocols
Finance	Financial policies
Governance	Incident planning for mass casualty Incident/emergency managers of mass casualty Incident committee for mass casualty Incident exercise/drill for mass casualty Incident command systems in a hospital Analysis of hazard vulnerability

Table 7. Main concepts and subconcepts of preparedness challenges in biological incidents/events in a hospital

Main Categories	Subcategories
Risk communication	Informing
	Perception of risk
Laboratory and surveillance	Laboratory detection capability
	Syndromic surveillance systems
Patient management	Treatment management
	Biological triage
Safety and health	Individual safety
	Environmental safety
Resource management	Surge capacity (equipment and structure)
	Staff management: *Organizational factors* *Motivational factors* *Individual factors*
Education and training	Scenic practices
	Inefficient training

Understanding preparedness challenges in a hospital against biological incidents/events such as COVID-19 is necessary to improve dynamics, quality, and BC confidence in a healthcare system. Main concepts and subconcepts have been extracted regarding preparedness challenges in biological incidents/events in a hospital, which is listed in Table 7 [17].

5. Business Impact Analysis in a Medical Center

Charleston Regional Medical Center is a large medical center/hospital that serves patients in Jackson, Mississippi, USA. When facing a critical data loss event, patient care processes may be categorized by attacks or incidents. Each incident or attack carries its criticality and must be judged according to how essential the attack or incident is to patient care. Each incident or attack must also carry its significant breach method in the data loss, for example, humans, computers, or networks must be identified to identify and correct the patient care process. Table 8 shows the names of incidents/attacks, their types, and their impacts (L: low; M: medium; H: high) on the Medical Center.

Table 8. Incidents/attacks, types, and impacts in the Medical Center

Incidents/Attacks	Types	Impacts
Email phishing	Computer systems	L
Ransomware	Computer systems	H
Attacks against non-essential medical devices	Network, Human, computer systems	L
Loss or theft of patient data	Human	H
Loss or theft of equipment	Human	H
Insider, accidental data loss	Human	M
Insider, intentional data loss	Human	H
Mobile device attacks	Human, computer systems	H
Attacks against networked key patient care equipment	Human, computer systems, network	H
Billing data attacks	Human	M

Based on the criticality level, the impacts of a business process can be mapped to the RTO, RPO, and maximum tolerable downtime (MTD). Any enterprise has its unique RTO and RPO needs. In a Medical Center, RTO and RPO are often very short due to the nature of the data recovery and the necessity for a return to patient care, which is often immediately to prevent death. Recovery point objectives normally combine with RTOs, or the anticipated time until an enterprise can return operations to normal after an event. Computer programs using RTO and RPO frequently guarantee critical data is replicated and stored accurately and is instantly accessible when it is needed. The primary distinction between RTO and RPO is that RTO connects to processes and patient care levels. Instead of a delay in retrieving data, an RTO tracks exactly how long a medical center may be able to exist without performing patient care tasks. Table 9 summarizes the result of BIA when the disruption of patient care processes occurs due to attacks in the Medical Center. The BIA result includes RTO, RPO, MTD, and the criticality level (L: low; M: medium; H: high).

Table 9. BIA results in the disruption of patient care processes in the Medical Center

Patient Care Processes	RTO (hours)	RPO (hours)	MTD (hours)	Criticality
Data center service (e.g., billing, insurance claims, research, etc.)	1	4	1	M
E-sign service	1	1	1	H
Patient records	1	1	1	H
Provider mobile devices	1	4	4	M
Key networked medical equipment (e.g., ventilators, IV pumps, heart rate monitors, defibrillators, etc.)	0	0	0	H
Non-essential networked medical equipment (e.g., non-patient care equipment, beds, call lights, etc.)	4	12	4	L

6. Conclusion

Enterprise administrators find it necessary to create a BCP to outline specific enterprise tasks and steps essential to the organization and critical to perform during and after a cyber event. A BCP created by the organization can improve steps taken by the IT Department before and after a service disruption because it analyzes organizational risk factors and improves the organization's readiness to resume regular operations after a current or future service disruption. A core component of the BCP is the BIA which is typically static and is based on current organizational priorities or the operations environment. However, to guarantee that the BCP is vigorous and adapts to changing conditions rapidly and easily, the BIA must consider any potential for change. Identifying knowledgeable staff and key administrators with the skills necessary to ensure information is accessible allowing for staff to cross-train also enhances resources for key roles. Another function of the BCP is planning a set of procedures that will allow the enterprise to quickly return to a fully functioning status in the event of a cyber-attack. Unfortunately, many businesses have a widely generalized business plan that will return the organization to full function. This is due to the lack of testing and flexibility within the BCP. Traditional approaches to the BCP must evolve to include new and previously untested tactics. An organization must also adapt or advance its BIA to guard against further cyber-attacks. A BIA becomes an effective and advanced tool for protecting the enterprise. In healthcare, the BIA is critical as it can help restore functioning to all levels of the facility. All types of events and levels of cyber-attacks should be prepared for by hospital administrators. Future research is a comprehensive risk assessment for healthcare, including both qualitative and quantitative evaluation; system-level vulnerabilities and losses; and cyber risks (internal and external risks) and their measurements, impacts, and likelihood.

ACKNOWLEDGEMENTS

The authors would like to express thanks to Technology and Healthcare Solutions, USA for its help and support.

Conflict of Interest

The authors would like to announce that there is no conflict of interest.

References

[1] Swanson, M. M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. (2010). Contingency Planning Guide for Federal Information Systems [including updates through 11/11/2010].

[2] Hatton, T., & Brown, C. (2021). Building adaptive business continuity plans: Practical tips on how to inject adaptiveness into continuity planning processes. *Journal of Business Continuity & Emergency Planning*, *15*(1), 44–52.

[3] Blass, G. (2021). Mitigate risk while preparing for the future: Why you need a DRBC Plan. *Journal of Health Care Compliance*, September–October.

[4] Yi, B., Sawant, A., Chen, S., Lee, S. W., & Zhang, B. (2022). Readiness for radiation treatment continuity: Survey on contingency plans against cyberattacks. *Advances in radiation oncology*, *7*(5), 100990.

[5] Burroughs, A. (2021). Keeping it together: Why tested business continuity plans are important in a crisis. *Smart Business Cleveland*, *32*(7), 30.

[6] Debra Cascardo, M. A. (2020). Learning to live with volatility: preparing for business continuity and recovery following a disaster. *Physician Leadership Journal*, *7*(4), 69-72.

[7] Lee, A., Vargo, J. and Seville, E. (2013). Developing a tool to measure and compare organizations' resilience. *Natural Hazards Review*, *14*(1), 29–41.

[8] Whitman, Z., Kachali, H., Roger, D., Vargo, J. and Seville, E. (2013). Short-form version of the Benchmark Resilience Tool (BRT-53). *Measuring Business Excellence*, *17*(3), 3–14.

[9] Tistiyani, S., Briliyant, O., & Trianto, N. (2023, August). Tailoring e-Government's ICT Readiness for Business Continuity based on Cyber-Risk Approach. In *2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs)* (pp. 1-8). IEEE.

[10] Williams, T., & Resto-Leon, M. (2023). Cracking the code: The keys to a successful business impact analysis. *Journal of Business Continuity & Emergency Planning*, *16*(4), 313-319.

[11] Horalek, J. (2023). Business Impact Analysis of AMM Data: A case study. *Applied System Innovation*, *6*(5), 82.

[12] Aghabegloo, M., Rezaie, K., Torabi, S. A., & Yazdani, M. (2024). Integrating business impact analysis and risk assessment for physical asset criticality analysis: a framework for sustainable operations in process industries. *Expert Systems with Applications*, *241*, 122737.

[13] Motevali Haghighi, S., & Torabi, S. A. (2020). Business continuity-inspired fuzzy risk assessment framework for hospital information systems. *Enterprise Information Systems*, *14*(7), 1027-1060.

[14] Sasaki, H., Maruya, H., Abe, Y., Fujita, M., Furukawa, H., Fuda, M., ... & Egawa, S. (2020). Scoping review of hospital business continuity plans to validate the improvement after the 2011 Great East Japan Earthquake and Tsunami. *The Tohoku Journal of Experimental Medicine*, *251*(3), 147-159.

[15] Ito, H., & Aruga, T. (2022). A conceptual framework to assess hospitals for disaster risk reduction in the community. *International Journal of Disaster Risk Reduction*, *77*, 103032.

[16] Goniewicz, M., Khorram-Manesh, A., Timler, D., Al-Wathinani, A. M., & Goniewicz, K. (2023). Hospital disaster preparedness: A comprehensive evaluation using the Hospital Safety Index. *Sustainability*, *15*(17), 13197.

[17] Aminizadeh, M., Farrokhi, M., Ebadi, A., Masoumi, G., Kolivand, P., & Khankeh, H. (2022). Hospital preparedness challenges in biological disasters: A qualitative study. *Disaster Medicine and Public Health Preparedness*, *16*(3), 956-960.