Implementation of ICT Continuity Plan (ICTCP) in the Higher Education Institutions (HEI'S): SUC'S Awareness and its Status

Chester L. Cofino[1], Ken M. Balogo[2], Jefrey G. Alegia[3], Michael Marvin P. Cruz[4],
Benjamin B. Alejado Jr.[5], Felicisimo V. Wenceslao, Jr.[6]
College of Computer Studies, Central Philippines State University, Kabankalan City, Philippines[1,2,3,4]
College of Industrial Technology, Negros Oriental State University, Dumaguete City, Philippines[5]
College of Information and Computing Studies, Northern Iloilo State University, Iloilo, Philippines[6]

***Abstract*—The purpose of this study was to assess the level of awareness of the management and the personnel within the academic institution and identify the implementation status of the ICTCP to the implementing SUCs. The researchers used the BCM Framework was utilized in this study as the model for identifying the level of awareness of the personnel within the institution about the ICTCP. The research respondents were the personnel employed in the different States, Universities, and Colleges (SUCs) within the province of Negros Occidental. The respondents were selected through random sampling, they were provided by a google form link to answer the survey questionnaire. A total of thirty-five (35) IT personnel were included in the study's sample size. It was found out that most SUCs have consistent ICT system uptime because they can continuously provide services; surprisingly, this is independent of an ICT business continuity plan. Most SUCs do not entirely implement their ICT business continuity plans. Lastly, it is recommended that SUCs can significantly enhance service delivery if ICT business continuity planning is taken seriously, adopted, and entirely carried out.**

Keywords*—Business continuity plan (BCP); information, communication; and technology continuity Plan (ICTCP); state universities and colleges (SUCs); business continuity management (BCM) framework

I. INTRODUCTION

The importance of technology for information and communication (ICT) as component of enterprises worldwide has become crucial. It comprises communication technologies, infrastructure, hardware, and software related to information systems. This technology and systems will eventually malfunction due to unexpected catastrophes or causes. The ICT systems must be recovered and put back into operation with the fewest possible downtimes because they are a crucial component of corporate functions. According to [1], the speed at which business operations recover guarantees that it will outperform its rivals and provide customers with a high degree of satisfaction.

In the Philippine setting, one of the legal bases is the Data Privacy Act of 2012 (RA10173), ensuring that all government institutions, like States, Universities, and Colleges (SUCs), will craft its ICT Continuity Plan (ICTCP) to protect their business process and provide excellent service to their clients. Furthermore, on March 24, 2020, Republic Act No. 11469, known as the "Bayanihan to Heal as One Act" was signed into law. In this regard, the DICT hereby directs all public telecommunication entities (PTEs) and government agencies, including academic institutions, to submit their Business Continuity Plan (BCP) and other measures to ensure uninterrupted service and to address the increased demand for ICT services.

In this regard, this study aimed to assess the level of awareness of the management and the personnel within the academic institution and identify the implementation status of the ICTCP to the implementing SUCs. Ascertain the extent of the use of computers using ICT at the State Universities and Colleges (SUCs) in Negros Occidental, Philippines. Ascertain how frequently the ICT systems SUCs relied on broke down and if the continuity plan is in place. Lastly, to ascertain how an ICT business continuity plan affected the provision of services.

II. RELATED WORKS

ICT business continuity planning is a system of practices, guidelines, and proactive preparation that guarantees the restoration of vital ICT-dependent services in an emergency [2]. It enables the company to make crucial strategic, tactical, and operational decisions on the availability of essential systems [3]. In preparation for any system outage, resources such as software, hardware, technical experience, monitoring, time, and other infrastructure are established during an ICT business continuity plan.

The implementation must be maintained periodically and managed adequately. However, some studies concerning IT Audit found that some of the existing Business Continuity Plan (BCP) that is not entirely and correctly updated and will fail the business to continue its operation when disruption happens [4]. This was also seconded by the study [2] that due to the ICT business continuity plan not being viewed as a strategic component of the company, it has not been completely implemented and was neglected. According to [5], many organizations did not feel the need to deal with the BCP in the past because the dependence on ICT was not so significant, and production could run for some time regardless of a data network in the organization.

BCP was beneficial for all of the organizations that were surveyed. Still, more focus is required on managing societal and individual impacts, building employee resilience, identifying influential crisis leaders, right-sizing plans, and planning to take advantage of opportunities after a disaster. It is also essential to assess employees' awareness of the general coordination of information technology regarding these processes [6].

III. IMPLEMENTATION

The study's general objective is to ascertain how ICT continuity plans affects on service delivery and assess the level of awareness of the personnel of State, Universities, and Colleges (SUCs) in the Philippines, specifically in Negros Occidental. Furthermore, it is to identify the advantages of an ICT business continuity strategy for SUCs in Negros Occidental**.** The study is based on the descriptive type, which involved a primary gathering of data from the respondents in terms of their profile and assessment of the availability of the ICTCP in their respective institutions.

A. The Business Continuity Plan (BCM) Framework

The BCM Framework was utilized in this study as the model for identifying the level of awareness of the personnel within the institution about the ICTCP (Fig. 1). The six elements of the BCM life cycle, according to the international standards, the management of the business continuity program, instilling knowledge and skills into the organizational culture, knowing the organization, choosing options for business continuity, creating and putting into practice a business continuity response, and practicing and testing the developed plans [7].

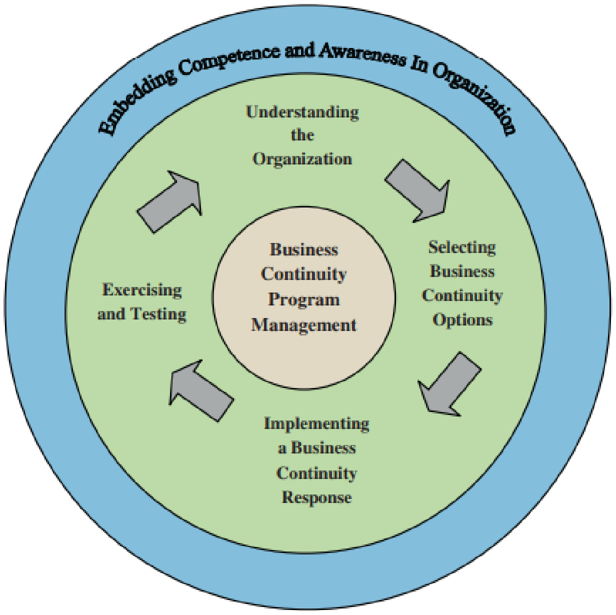
Embedding Competence and Awareness In Organization
Understanding the Organization
Selecting Business Continuity Options
Implementing a Business Continuity Response
Exercising and Testing
Business Continuity Program Management

Fig. 1. The lifecyle of BCM [7].

B. Understanding the Organization

According to [8], the outcomes of the BCP implementation show that all framework components can be implemented, but some activity changes must be made to suit the organizational conditions. Personnel in the organization must be aware of the implementation because they are the ones providing the services. This component aims to offer crucial details that will aid in understanding the company's goods, resources, and services [9]. Furthermore, the principal target objective, specific objectives, and policy are visible and disseminated to the employee from the top management to the office personnel.

Table I presents the role and responsibilities of the BCP team for SUCs. The team composed of the top management who see to it the requirements, budget allocation, and implementation of the ICTCP would be successful.

TABLE I. ROLE AND RESPONSIBILITIES FOR BCP TEAM

BCP Member	Roles
BCP Manager	• Ensures that the ICTCP is established, maintained, and reviewed periodically. • Approves allocation of resources to ensure successful implementation of the plan.
Vice President for Administration and Finance	• Ensures implementation and compliance with the ICTCP. • Ensures the continual improvement of the ICTCP.
Planning Officer	• Consolidates and evaluates personnel needs required to ensure the continuity of ICTCP critical unit functions and operations. • Ensures continual improvement.

Table II shows the composition of the ICT Response Team. The team must ensure that the ICTCP implementation is successful. The SUCs may designate a working team with expertise in ICT.

TABLE II. ROLE AND RESPONSIBILITIES OF ICT RESPONSE TEAM

Member	Roles
IT/MIS Officer	Establish, implement, and maintain a continuity of the ICT Business Operation of the University.
Data Privacy Officer	Inform and provide advice on data protection obligations, assist the University in monitoring internal compliance.
System Administrator	System administrators are the guardians of an organization and its data, ensuring that internal systems are safe and secure and are shielded from attacks and viruses.
Network Administrator	Ensuring ICT equipment remains updated and providing solutions to restore functionality.
Development Communication and Information Officer	Consolidates, controls, and validates all official information for dissemination. Creating information, education, and communication (IEC) items in both English and regional dialects.

C. Selecting Business Continuity Options

Threats could appear out of nowhere at any time. Business continuity management is necessary to prepare for and address the problem. The last step in completing business continuity management is the requirement for a framework for a business continuity strategy. This framework will guide the organization using the business continuity plan document to address threats or disasters [10]. Good decision on what framework to adapt is vital for the success of the implementation of the ICTCP.

D. Implementing a Business Continuity Response

According to [11], the fundamental idea behind business continuity is that to maintain company operations at an acceptable level, an organization must have the strategic and tactical capabilities to plan for and respond to business accidents and disruptions. Readiness is also vital in implementing a business continuity plan from management perspective and fulfilling the gap existing with a business continuity plan using a standard tool [12]. Many SUCs appear unfamiliar with and uncertain about which Business Continuity Management (BCM) option can be used for implementation. Organizations are becoming increasingly aware that being unprepared to handle disruptive occurrences could have disastrous results. BCM is a novel strategy to accomplish this goal. When a BCM is implemented in a company, there are three primary stages that need to be taken. The key items for the company should be recognized first. The Business Impact Analysis (BIA) technique can assist in this step by assisting in the systematic selection of those crucial products. Second, by carrying out the risk assessment process and creating the risk matrix, those risks that endanger the delivery of crucial products should be recognized and categorized. Finally, a BCP must be chosen for each disruption risk listed in the BCP section of the risk matrix and poses a danger to a significant product [13].

IV. Results

The research respondents were the personnel employed in the different States, Universities, and Colleges (SUCs) within the province of Negros Occidental. The study utilized an adopted questionnaire from the study [2] on ICT Business Continuity Plan and Service delivery.

The respondents were selected through random sampling, they were provided by a google form link to answer the survey questionnaire. A total of fifty (50) people were included in the study's sample size. As shown in Table III, fifteen (15) from Central Philippines State University, ten (10) from Northern Negros State College of Science & Technology, fifteen (15) from Carlos Hilado Memorial State University, and ten (10) Technological University of the Philippines – Visayas.

A scale of 1 to 5 was used based on the Likert scale, and a non-comparative scaling approach was used.

The study expected a target of 50 respondents to answer the survey questionnaire. However, 35 of the estimated number filled out the surveys and returned them. Thus, as shown in Table III, the answer rate was 70%. This response rate was deemed suitable for analysis since, according to [14], a minimum of 70% or higher is exceptional for analysis.

TABLE III. Distribution of Respondents

SUC	Expected Reponses	Percentage	Responses Received	Percentage
Central Philippines State University	15	30.00	15	42.90
Northern Negros State College of Science & Technology	10	20.00	5	14.29
Carlos Hilado Memorial State University	15	30.00	10	28.58
Technological University of the Philippines - Visayas	10	20.00	5	14.29
Total	50	100.00	35	100.00

V. Discussion

A. Use of ICT

The purpose of the study was to ascertain the extent of the use of computers using ICT at the State Universities and Colleges (SUCs) in Negros Occidental, Philippines, which necessitated the creation of a business continuity plan for ICT. According to Table IV below, 0% of respondents did not rely on ICT for all their key operations, whereas 100% used ICT for all their essential duties. The value of information and communication technology (ICT) in education is unquestionable on a global scale. It has the potential to be very effective to use ICT to increase educational opportunities. ICT has the potential to improve the relevance and standard of education while expanding access to it [15].

TABLE IV. Extent of ICT Usage

Responses	Frequency	Percentage
Yes	50	100.00
No	0	0.00
Total	50	100.00

B. Failure of ICT core systems

The study aimed to ascertain how frequently the ICT systems SUCs relied on broke down. According to Table V below, 82.6% of respondents said their systems failed only occasionally, while 17.4% said it happened sometimes. 33.1% of the respondents reported that system failure-causing disasters never or only occasionally happened, compared to 45.6% who experienced disasters sparingly and 21.3% who never experienced system outages due to disasters. According to [16] it is crucial to improve their capability for ICT policy, respond to shifts in the ICT ecosystem, develop robust cybersecurity regulations, and make sure the private sector operates under predictable conditions.

TABLE V. FAILURE OF ICT CORE SYSTEMS

Responses' Percentage Distribution					
System Failures	Never	Rarely	Sometimes	Always	Total
Your systems fail frequently.	0.0%	82.6%	17.4%	0.0%	100%
Disasters occur, causing system outages	21.3%	45.6%	33.1%	0.0%	100%

C. Access to the ICT Continuity Plan

The study aimed to ascertain whether the four SUCs in the Philippine province of Negros Occidental had an ICT business continuity plan in place to lessen or avert the results of system malfunctions brought on by emergencies. Table VI demonstrates that only 2 SUCs had an ICT business continuity plan compared to the other 2 SUCs. Maintaining organizational operations in the face of potential threats, risks, the causes of power outages, cyberattacks, or epidemiological attacks, or natural disasters. BCP is therefore crucial in SUCs to plan for any risk [17].

TABLE VI. AVAILABILITY OF ICT CONTINUITY PLAN

Responses	Frequency	Percentage
Yes	2	50.00
No	2	50.00
Total	5	100.00

D. Availability of ICTCP Policies

The study looked into any internal guidelines for managing, regulating, and controlling the ICT business continuity plan. This was done to assess the level of implementation of ICT business continuity plans (Table VII). Two SUCs had established policies, while the other two did not.

TABLE VII. AVAILABILITY OF ICT BUSINESS CONTINUITY PLAN POLICIES

Responses	Frequency	Percentage
Yes	2	50.00
No	2	50.00
Total	4	100.00

E. Availability of Disaster Recovery Site

The study examined whether it was possible to check the effectiveness of the ICT business continuity plan at an off-site location for disaster recovery. One SUC lacked a recovery site, while the other three had them to help with recovery (Table VIII).

TABLE VIII. SITE FOR DISASTER RECOVERY IS ACCESSIBLE

Responses	Frequency	Percentage
Yes	3	75.00
No	1	25.00
Total	4	100.00

F. Challenges of ICTCP

The study aimed to identify the problems and develop an ICT business continuity strategy for the SUCs in the Philippine province of Negros Occidental. Table IX below shows that responses with a mean of 4.52 demonstrated strategies fail due to insufficient resources. With a standard of 3.80, respondents responded that the ICT plan requires an extensive planning for the second significant difficulty, and stakeholders in the firm do not have access to enough information concerning ICT business continuity plans. Limited resources were rated as the main obstacle to an ICT business continuity plan by 2.6. The institution's ICT strategy is not seen as a strategic component, according to respondents with a mean score of 2.41. According to respondents, with a mean of 2.57, the ICT business continuity plan is seen as an ICT-only job that excludes other departments. A standard of 2.5 respondents revealed that managing the ICT business continuity plan required technical competence and that stakeholders were not properly informed about what an ICT business continuity plan involved inside the organization.

TABLE IX. ICT BUSINESS CONTINUITY PLAN CHALLENGES

Items	N	Mean	Std. Deviation
ICT plans fail as a result of insufficient resources.	35	4.52	.936640
Plans for ICT business continuity need to be carefully thought out.	35	3.80	1.222376
The company's stakeholders are not adequately informed about what an ICT business continuity plan entails.	35	3.80	1.222376
The amount of time required to implement an ICT business continuity plan is excessive.	35	2.57	.654970
ICT business continuity plans cannot be updated as quickly as technology does.	35	2.40	.932764
ICT systems experience system failures more frequently than earlier manual processes, necessitating ongoing monitoring.	35	2.65	1.139540
The institution does not view the ICT business continuity plan as a strategic component.	35	2.40	.932764
The management of an ICT business continuity plan requires technical expertise.	35	2.50	.781736
There are no regulations in place to support the administration of the plan.	35	2.97	.987849
According to some, the ICT business continuity plan only pertains to ICT and excludes other departments.	35	2.57	.654970

G. Service Delivery

The study's goal was to ascertain how an ICT business continuity plan affected the provision of services. Table X demonstrates that the companies' profit margins increased as a result of customer satisfaction for the SUCs was based on the quality of services offered, offered superior goods and services with a mean of 3.57, and with a mean of 2.57, service delivery was boosted through the institution's adoption of an ICT business continuity plan.

TABLE X. SERVICE DELIVERY

Items	N	Mean	Std. Deviation
Customer satisfaction depends on how well services are provided.	35	3.57	1.184644
Service delivery is improved thanks to our company's adoption of an ICT business continuity plan.	35	2.57	.654970

VI. CONCLUSION

The study found out the advantages of an ICT business continuity plan that most SUCs believed it benefited from the shortened time needed for system recovery after a failure. Other advantages were the development of teamwork and system understanding through employee engagement plans, the realization, and reduction of points of failure during the testing of the ICT business continuity plan, the ability to know what to do in the event of a disaster, reduction of losses caused by unforeseen disasters, effective resource planning for the company in the event of a disaster.

According to the study's findings, ICT has been widely adopted in SUCs, and it is clear that these institutions need their systems to operate continually with little chance of failure. Most insurance businesses implement an ICT business continuity plan to ensure fewer system disruptions and downtimes. Most SUCs have consistent ICT system uptime because they can continuously provide services; surprisingly, this is independent of an ICT business continuity plan. Most SUCs do not entirely implement their ICT business continuity plans. The ICT business continuity plan was easily overlooked or misunderstood as an ICT role because it had not been considered a strategic business need. It was also found to be resource-intensive and time- and planning-intensive.

The study's conclusions allow for the following recommendations: SUCs can significantly enhance service delivery if ICT business continuity planning is taken seriously, adopted, and entirely carried out. This is due to several reasons, including that they impact how services are delivered. An ICT business continuity strategy will ensure that ICT systems are always accessible to prevent service disruptions.

The proper management of ICT business continuity plans requires clearly defined rules, guidelines, and policies, efficient testing intervals, the availability of disaster recovery sites, enough time, hardware, software, and technology resources, as well as technical expertise and teamwork.

ACKNOWLEDGMENT

The researchers would like to thank Dr. Felicisimo V. Wenceslao, Jr. , professor of College of Information and Computing Studies at the Northern Iloilo State University, for introducing us to this topic and providing invaluable guidance and support during the research.

REFERENCES

[1] S. Li and Y. Yan, "Data-driven shock impact of COVID-19 on the market financial system," Inf Process Manag, vol. 59, no. 1, Jan. 2022, doi: 10.1016/j.ipm.2021.102768.

[2] H. Kavonga, "ICT Business Continuity Plan And Service Delivery In Insurance Companies In Kenya A Project Submitted In Partial Fulfillment Of The Requirements For The Award Of The Degree Of Master Of Business Administration (Mba), School Of Business, University Of Nairobi 2017."

[3] M. Niemimaa, J. Järveläinen, M. Heikkilä, and J. Heikkilä, "Business continuity of business models: Evaluating the resilience of business models for contingencies," Int J Inf Manage, vol. 49, pp. 208–216, Dec. 2019, doi: 10.1016/j.ijinfomgt.2019.04.010.

[4] J. Hagelbäck, "Hybrid Pathfinding in StarCraft," IEEE Trans Comput Intell AI Games, vol. 8, no. 4, pp. 319–324, Dec. 2016, doi: 10.1109/TCIAIG.2015.2414447.

[5] M.-A. Kaufhold et al., "Business Continuity Management in Micro Enterprises: Perception, Strategies, and Use of ICT," International Journal of Information Systems for Crisis Response and Management, vol. 10, no. 1, pp. 1–19, Jan. 2018, doi: 10.4018/ijiscram.2018010101.

[6] E. D. Canedo et al., "Information and communication technology (ICT) governance processes: A case study," Information (Switzerland), vol. 11, no. 10, pp. 1–28, Oct. 2020, doi: 10.3390/info11100462.

[7] S. A. Torabi, H. Rezaei Soufi, and N. Sahebjamnia, "A new framework for business impact analysis in business continuity management (with a case study)," Saf Sci, vol. 68, pp. 309–323, 2014, doi: 10.1016/j.ssci.2014.04.017.

[8] S. V. Fani and A. P. Subriadi, "Business continuity plan: Examining of multi-usable framework," in Procedia Computer Science, 2019, vol. 161, pp. 275–282. doi: 10.1016/j.procs.2019.11.124.

[9] E. Fasolis1, V. Vassalos2, and A. I. Kokkinaki3, "IFIP AICT 399 - Designing and Developing a Business Continuity Plan Based on Collective Intelligence," 2013.

[10] S. Fani and A. Subiadi, "Trend of Business Continuity Plan: A Systematic Literature Review," Feb. 2020. doi: 10.4108/eai.13-2-2019.2286164.

[11] N. Russo, L. Reis, C. Silveira, and H. S. Mamede, "Framework for designing Business Continuity-Multidisciplinary Evaluation of Organizational Maturity," in Iberian Conference on Information Systems and Technologies, CISTI, Jun. 2021. doi: 10.23919/CISTI52073.2021.9476297.

[12] G. Pramudya and A. N. Fajar, "Business Continuity Plan using ISO 22301:2012 in it Solution Company (PT. ABC)," In It Solution Company (Pt. Abc) International Journal of Mechanical Engineering and Technology, vol. 10, no. 2, pp. 865–872, 2019, [Online]. Available: http://www.iaeme.com/IJMET/index.asp865http://www.iaeme.com/ijmet/issues.asp?JType=IJMET&VType=10&IType=2http://www.iaeme.com/ijmet/issues.asp?JType=IJMET&VType=10&IType=2

[13] H. Rezaei Soufi, S. A. Torabi, and N. Sahebjamnia, "Developing a novel quantitative framework for business continuity planning," Int J Prod Res, vol. 57, no. 3, pp. 779–800, Feb. 2019, doi: 10.1080/00207543.2018.1483586.

[14] A. G. and A. M. Mugenda, "Qualitative research methods," 2013.

[15] K. Das, "International Journal of Innovative Studies in Sociology and Humanities (IJISSH) The Role and Impact of ICT in Improving the Quality of Education: An Overview," 2019, [Online]. Available: www.ijissh.org

[16] T. Corrigan, "African perspectives Global insights Policy Briefing 197 Africa's ICT infrastructure: Its present and prospects," 2020. [Online]. Available: https://www.afdb.org/en/knowledge/publications/tracking-africa%E2%

[17] N. Roxana Moşteanu Professor, "Article ID: IJM_11_04_018 Cite this Article: Dr. Narcisa Roxana Moşteanu, Management of Disaster and Business Continuity in a Digital World," International Journal of Management, vol. 11, no. 04, pp. 169–177, 2020, [Online]. Available: http://www.iaeme.com/IJM/index.asp169http://www.iaeme.com/ijm/issues.asp?JType=IJM&VType=11&IType=4JournalImpactFactor