Evaluation of Business Continuity and Information Disaster Recovery Mechanism in Top Universities in North Cyprus

Victor Legbo YISA, Meshach BABA

***Abstract*— the importance of a business continuity and disaster recovery plan to an organization cannnot be over-emphasised. Business continuity in an organization serve as a lifeline to organizations when a disasteer event occurs. This study emphasises on the need for an effective business continuity and disaster recovery plan in higher education institutions by evaluating universities in north cyprus' disaster recovery mechanism.Deming circle approach was used in evaluation with questions asked to respondents based on the four different stages of the Deming circle.**

***Index Terms*— Business Continuity, Deming Circle, Disaster, Disaster Recovery.**

I. INTRODUCTION.

In every organization, unexpected and undesired circumstances may arise that may hinder normal business processes and may cause either a temporal or permanent shut down of the business, this circumstances are business threatening and are called disasters. Disasters could be man-made or naturally caused. Because of the spontaneous nature of disasters, there is need for a clear contingency plan on how the organization should be run in case of a disaster, there should be a precise description on how the organization can keep running its business in case of a disaster. Also there should be a defined plan on how the organization can recover from the disaster and resume normal operations.

Business Continuity Planning and Disaster Recovery Planning involve the preparation, testing, and updating of the actions required to protect critical business processes from the effects of major system and network failures. Business continuity plans are created to prevent interruptions to normal business activity. A disaster recovery plan is a comprehensive and coordinated statement of consistent actions to be taken before, during, and after a disruptive event that causes a significant loss of information systems resources.

II. THE RESEARCH PROBLEM

North Cyprus a Mediterranean country has recently become famous as a great education destination, students from all around the world (Europe, Asia and Africa) come to north Cyprus for their undergraduate and postgraduate degrees owing to the fact of them obtaining quality education from the schools, also information systems have embedded deep into every aspects of the schools department. student application, records, accommodation, provision of internet, the schools accounting department, security department, student registration, learning materials, modules, mails etc all make use of the information system. The Cyprus International University library has more eBooks and e-journals than the physical hard copy of books. Webservers are used for by the schools website; huge mail servers host the school webmail. Almost all the schools activities make use of information technology systems powered by electricity. Due to natural or man-made occurrences, this systems that are critical to the schools might become unusable, therefore the need for a contingency plan that will see that normal activities continue until the systems get back running.

Manuscript Received on September 22, 2014.

Victor Legbo Yisa, Department of Cybersecurity Science, Federal University of Technology, Minna, Niger State, Nigeria.

Meshach Baba, Department of Cybersecurity Science, Federal University of Technology, Minna, Niger State, Nigeria.

III. AIMS AND OBJECTIVE

The study aims to analyze and evaluate the business continuity and disaster recovery plan of selected top universities in North Cyprus.

IV. RESEARCH QUESTIONS

The research will try to address issues in the aforementioned case study areas like:

1. Is there a business continuity/disaster recovery plan?
2. Is there a BC/DR team/committee in these schools?
3. Are all stakeholders considered when making a BC/DR plan?
4. What are the estimated downtime that could be accommodated for internet and power?
5. When last was a BC/DR plan tested?
6. How regular are the plans tested?
7. Has it ever been revised?
8. When it was last revised?

V. LITERATURE REVIEW

A. Introduction.

"He who fails to plan, plans to fail" goes a wise saying, a business that fails to have a contingency plan for the rainy days will find itself in sinking muddy waters when the bad days come. There is need for a backup plan, a plan that will help the business to be operational and serve as a guide to an organization when adverse uncertain situations arise.

Kingdoms from ancient times would prepare against adverse conditions by building

forts, strong walls, food storages, water storages, canals andalliances with other kingdoms. Whenadverse situations arise like a war with hostile kingdom, the kingdom relies on past preparations it has made to keep it running despite the attacks from its enemies. The storage feeds the people, the walls and forts keep the enemy out and its army tries to fight the enemy such that things will return back to normal again. Also, the kingdom could rely on its other town for economic support if the major town is under attack. The scenario discussed above is akin to what business continuity and disaster recovery is to organizations of the present era.

A business is not just an enterprise or firm, a business can be defined as the various processes, activities, people, product and services [1]. Another definition of business continuity is the continuation of business processes when uncertain adverse situations arise. These situations could be epidemic diseases, natural disasters, technology failure, accidents, cyber-attacks, terrorism and any other circumstance that could cause disruption to business activities. The major aims of business continuity are:

1. The business critical functions should be sustained in compliance with standard regulations and deliver its product and services with minimum losses
2. Ensure the customer is attended to with satisfaction so that customers are made and business reputation is built and maintained.

Business continuity planning can be defined as a strategy to minimize the effect of disturbances and to allow resumption of normal business processes [2] and [3]. It is important that every business and organization have a disaster recovery plan as it is certain that they will encounter disruptions in one way or the other. Business continuity planning (BCP) is the act of expecting adverse uncertain situations that could cause disruptions to occur, and making sure they are prevented or their chances of occurrence is reduced, and if they do occur, an appropriate response in a planned and organized way is used to mitigate their effect such that the business does not suffer heavy losses and is recovered back from the situation so that normal business processes are resumed. Due to the advancement of Information Technology (IT), business nowadays depends heavily on IT.

With the advent of the internet, the computing need in organizations skyrocketed, almost every single activity is computerized, and organizations relied completely on the continuous availability of information systems[4]. This need of keeping the systems up and running all the time increased the awareness of having a proper disaster recovery and business continuity plan. Also increasing natural disasters like earthquakes, floods, tsunamis etc. increased the need for such plans.

A man-made disaster such as the September 11 attacks in 2001 was estimated in the national accounts to cost about $14 billion for private businesses, $1.5 billion for State and local government enterprises and $0.7 billion for Federal government in the United States [5].

With the emergence of e-business, many businesses can't even survive without operating 24Hours per day and 7 days a week. A single downtime might mean disaster to their business. This adverse uncertain negative situation that might occur is termed disasters. A number of authors have stated that about 60 percent of business that experience a major disaster such as fire close within two years, other statements are that a figure as high as 25 percent of businesses do not reopen after a major disaster such as fire. 75 percent of business fail within 3 years of been hit by a disaster. Such figures show how important business continuity and disaster recovery is for business organizations although Baird in the publication The Recovery Phase of Emergency Management insist that there is no any credible lead that such research that gave such figures had actually been carried out[6].The real source of such statistical figures remains elusive [7]. There has been an increasing awareness to the need for business continuity and disaster recovery plan by organizations, between the years of 2003 to 2006 there was an increase in budget spending on business continuity and disaster recovery by 25 percent [8].

Disaster recovery is defined as a set of activities coordinately executed after a disaster occurrence and making use of a backup facility that had allowed information technology users the access to important files needed to sustain the business during the disaster period [9] and [10]. Disaster recovery is the process policies and procedure related to continuation of the critical technological infrastructure due to a man-made or natural disaster [3]. Usually disaster recovery is implemented after the disaster had occurred. The major aim of disaster recovery is to make sure that every available action is taken to recognize and mitigate all forms of risks that might occur. An ideal disaster recovery plan is that that will never be implemented.

The term disaster recovery is a subset of business continuity and should be embedded in the general business continuity plan. A disaster recovery management system is the continuous process of planning, testing and the implementation of disaster recovery procedures such that in the event of an uncertain adverse situation vital the proper functioning of vital business operations.

Major elements of business continuity are as shown below [1].

1. Business impact analysis (BIA)
2. Risk management
3. Incident handling
4. Disaster recovery and restoration

B. Business impact analysis

One of the most important components of a business continuity plan, includes an in-depth analysis of the business processes to reveal the most critical of the processes, the most vulnerable (vulnerability assessment), risk analysis, and a plan to develop methods and policies to mitigate the risk and vulnerabilities. The BIA assumptions is that although every business activity is related and interwoven with another activity, there are still some very important processes that are very critical to the operation of the business[11]. The most critical processes are said because of their importance should be allocated more funds and attention than the less important business processes. One of the major function of the BIA is the identification of this business processes and determine which is more important to normal business functioning.

C. Risk management

Risks are unwanted uncertain incidents that could occur; they could be in form of a threat. Risk management is the process of identifying, evaluating and scrutinizing every aspect of an organization continuously and then effectively seeking ways to mitigate the identified risk [12]. The risk management process is made up of

1. Risk identification
2. Analysis
3. Prioritization
4. Planning
5. Mitigation
6. Monitoring
7. communication

Risk could be as a result of uncertainty in the industry, natural causes, accidents deliberate attack from rivals or any random event that could cause adverse conditions to the business.

Risk management is a continuous process and should never be stopped [13]. An organizations risk management committee continuously monitors the organizational events so as to be able to identify new risk and newer methods of mitigating them. Also constant monitoring of known risk is very important as this will help in taking mitigating actions even before the risk is induced into the system.

D. Incident handling

Once any disruption occurs an organization must know how to handle the situation immediately. This is called incident handling [1]. Although the risk management team could be doing their job, some disaster situations might arise and disruptions might occur of the processes [1]. When such disaster situation arises, knowing what to do to handle the circumstances immediately is called incident handling. Incident handling is a plan set out for dealing with disaster events such as cyber-attacks, fire, floods, and any other adverse situation in an organization

E. Disaster Recovery and Restoration

In the event of a disaster situation, the disaster recovery plan is implemented so as to recover the business to its original state before the disaster. A very important theory in disaster recovery planning is that there should be a backup site which should be physically separated from the primary site [4]

F. The Backup Site

Because a primary site is used for a business process is made unusable due to some disaster event. Business organizations make use of backup sites so that some critical business processes are continued in the case of a disaster in its primary site. The backup site choice and operation could be classified as follows depending on the nature of the business. Hot site, Warm site, Cold site [2].

***Hot site*:** described as the Cadillac of disaster recovery alternate backup sites, a hot site is that with all computing facilities installed with power, heating, cooling systems, functioning servers and workstations [2]. Up to date backup is done on the servers and workstations such that it is a replica of the actual primary business site. a hot site can provide availability of business processes in a matter of minutes in case of a failure at the primary site[4]. This type of site requires constant maintenance of the hardware software, data, to ensure the site is actually a mirror of the primary site.

One of the major advantages of the hot backup site is that it is available for use with all the necessary hardware and software capabilities at any particular point in time. A business with a hot site as a backup site will be able to survive disruptions to its critical processes in the primary site.

Cold site:A cold site is a similar type of disaster recovery service that provides office space, but the customer provides and installs all the equipment needed to continue operations. A cold site is less expensive, but it takes longer to get an enterprise in full operation after the disaster.

A cold site is a backup site that provides an empty space for installation of equipment needed for continue operation of the business once the initial primary site is rendered unavailable due to a disruptive disaster event. The cold site is a room ready for equipment to be installed with power already installed; heating and cooling systems are also installed. Sometimes communication facilities might be already deployed but it is not always the case. It is the most common form of backup site locations. Usually it takes a longer time for a cold site to come up, as system hardware will have to be deployed and configured, also necessary backups will have to be done, this makes a cold site take a longer time before it is up and running. Most business organization of recent times will have suffered a huge set back as a result of that as most oftheir business processes is done with computing resources. A downtime of some minutes might cost some business organizations millions of dollars aside making them loose clients and reputation. Another disadvantage of a cold site is that until a disaster really strikes, one cannot really tell if the cold site will ensure business continuity or not and maybe when it strikes it might be too late.

Warm sites:Warm site is that site that is a tradeoff between hot and cold site. It already has some hardware deployed. These hardware's represent some of the hardware you originally find in your primary site. Before the site is considered up and running the last backup from the primary site will have to be deployed on the computers

Although might be the most expensive approach to disaster recovery and business continuity, a hot site is the best alternative of the three

Backup Sites Services Could Be From

- Other locations owned and operated by the organization
- Companies providing disaster recovery services
- Agreement with other organizations in the sharing of computing and data facilities in the event of a disaster.

G. Business Continuity in Educational Environment

Most people's perception about business continuity is that it is meant for business firms or profit making organizations alone, but business continuity should be implemented in every organization that wants to succeed and continue operations as disaster situations can arise anytime and anywhere. Educational institutions and

nonprofit organizations need to start implementing business continuity as a disaster situation will lead to breakdowns in academic activities, significant financial losses, stalling of research projects[14]. Most higher educations have now deployed information's systems in their operations to help them deliver their services in an efficient and effective manner.Higher educational institutes now extremely rely on enterprise information system and all other related forms of information technology; this has raised the need for continuous service quality, availability and reliability in schools [15]. This continuous need was strengthened by a survey by the results of the twelfth annual EDUCAUSE Current Issues Survey [16] which opined that business continuity and disaster recovery ranks number nine in top ten information technology issues of institutions. EDUCAUSE argued that ongoing domestic and international disasters have generated an increase in such needs.

All institutions need that academic services are maintained and remain undisrupted when disrupting circumstances occurs. This can only be done if the institution has a comprehensive disaster recovery plan

Although there have been a number of research in educational institutes business continuity around the globe, north Cyprus institutes based on my findings have not really been researched on for business continuity planning and readiness for disasters. Maheshwari, et al, (2010) in their publication in the Disaster Recovery Journal suggested the PDCA (Plan, Do, Check, Act.) model for the development of a business continuity plan in Educational institutes [14]. The simplicity of the model and its widespread coverage of almost every area of the business continuity model is the more reason this model is adopted for this study. Survey questions will be grouped into Plan, Do, Check, Act and then the institutions business continuity is evaluated based on PDCA.

VI. Research Methodology

Primary data related to business continuity and disaster recovery mechanisms in higher educational institutions are obtained from the chief information officers (IT managers) of various schools in north Cyprus. The Deming circle is chosen to evaluate the business continuity and disaster recovery mechanisms of schools as it's a four stage change management process used by organizations for continuous improvement. It is also called the PDCA circle, and is made up of four basic stages:

1. Plan
2. Do
3. check
4. act/adjust

Because a BC/DR plans is considered a continuous process that needs to be improved upon, the Deming circle model which is best for iterative problems solution is used in the evaluating the schools business continuity and disaster recovery. Some survey questions are grouped into plan, do, check, and act in such a way that questions asked will help paint the schools business continuity and disaster recovery mechanisms.

The respondents are the schools chief information officers (IT managers) of the chosen schools. Although the questions were grouped into the PDCA, IT managers were unaware of this grouping and were just asked to give a precise answer to the questions and maybe give other comments where necessary. A total of 20 questions were thrown the respondents from both schools and their answers were noted. Once the questions are answered, the responses gotten are then analyzed by percentage ratings to each question.

A. Access to respondents

After a persistent contact with the respondents, interviews were scheduled. The researcher explained to them the relevance of the interview and how the results from them will be totally rendered anonymous which was essential to the progress of the research.

B. Study Area

There is an increasing popularity for higher educational institutions located in the Turkish republic of North Cyprus. Students all over the world are choosing Cyprus as their destination for quality education. Aside quality education, these schools provide state of the art IT facilities on campus for students.

Table 1List of Universities in North Cyprus

Name	Location	Established since
Eastern Mediterranean University	Famagusta	1979
Girne American University	Girne	1985
Near East University	Lefkosia	1988
European University Of Lefke	Lefke	1989
Cyprus International University	Lefkosia	1997
Middle East Technical University	Guzelyurt	2005
University Of Mediterranean Karpasia	Lefkosia	2010
Istanbul Technical University	Famagusta	2011

Out of the above mentioned schools, out of the above schools mentioned, visiting all the schools were a constraint due to financial reasons, another constraint that prevented that not all the schools were used is that not all of the CIOs were ready to give out such information as they felt some of the information might be sensitive. The prepared interview questions were administrated to the IT manage of two schools physically while a survey page containing the questions was prepared and the link sent through emails to the CIOs (IT managers) of other schools. A total of three CIOs responded to the online survey out of the

administered 6. Taking the number of schools surveyed to five out of the total eight of the universities. The schools chosen are remained anonymous as was the agreement with the respondents. The respondents were only willing to give the information agreeing that I do not give their names or the names of the school. The results from these schools are collected and assembled together making each school anonymous (will not mention any schools name) as was my agreement with the CIOs before they could give the answers. The data gathered from the research will be a better representation of the whole population of schools.

C. Structure of the interview questions

The Deming circle is chosen to evaluate the business continuity and disaster recovery mechanisms of schools as it's a four stage change management process used by organizations for continuous improvement. It is also called the PDCA circle, and is made up of four basic stages:

1. Plan
2. Do
3. check
4. act/adjust

The interview questions were structured into the four stages of the Deming circle, Plan, Do, Check, and adjust/act.

Out of the 20 questions thrown at the respondents, three were questions aiming to test organizations planning procedure for BCP/DRP. Ten of the questions are used in the evaluation of the Do section of the Deming circle which access what the organization has done to ensure business continuity. The following four question asked to the respondents are used in evaluating to check how effective the do section has been. The last two questions are asked to know if the lessons learnt from the check is used to adjust the plan for better results.

This method is used because business continuity is an iterative process and to measure the effectiveness of the business continuity and disaster recovery mechanism of each school. Although some of the questions were open ended questions, most of the questions were structured in a way that the respondents answer yes or no or partially, also for each question respondents were allowed to make any comment of their perception about the question.

VII. RESULTS

Results from each of the questions are evaluated based on a percentage school to see if the schools responses are akin to international standards. Responses under the PDCA groupings are then analyzed to see how schools faired under the groupings.

Here is a summary of the results that includes the response count, and the response percentage.

Table 2Results for the plan stage

s/n	PLAN		Response percentage	Response count
1	The top management clearly understands the need for business continuity and disaster recovery plan, funds and takes care of every activity that will take place throughout the planning process.	Yes	60%	3
		No	0%	0
		Partially	40%	2
2	Does the institution have a budget allocated for business Continuity and disaster recovery?	Yes	20%	1
		No	0%	0
		partially	80%	4
3	Does the business continuity planning team/committee have representatives from every functional section of the institution?	Yes	40%	2
		No	20%	1

Table 3Results for the Do Section

	DO		Response percentage	Response count
1	Have you engaged with local emergency responders to develop plans for helping your organization and your community during an emergency?	YES	40%	2
		NO	0%	0
		PARTIALLY	60%	3
2	Has the Team accessed risk to the institution and taken necessary precautions to protect the institution?	YES	100%	5
		NO	0%	0
		PARTIALLY	0%	0
3.	Does your business continuity plan include people, premises, technology, information and stakeholders?	YES	60%	3
		NO	20%	1
		PARTIALLY	20%	1
4	Are all stakeholders (including staff	YES	20%	1
		NO	0%	0

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

	and students) aware of a business continuity procedure and aware of what to do in case of a disaster event?	PARTIALLY	80%	4
		.		
5	What is the maximum tolerable outage (MTO) for a power disruption the institution can accommodate?	0-6hrs	20%	1
		6-24hrs	20%	1
		1-3days	40%	2
		3-7 days	0%	0
		over 7days	20%	1
6	What is the maximum tolerable outage (MTO) for internet connectivity the institution can accommodate?	0-6hrs	0%	0
		6-24hrs	20%	1
		1-3days	20%	1
		3-7 days	20%	1
		over 7days	40%	2

Table 4: Results for the check Section

s/n	CHECK		Response percentage	Response count
1	How often do you conduct a Business Continuity/Disaster Recovery test in the institution?	less than a year	75%	3
		1 to 2 years	25%	1
		3 to 5 years	0%	0
2	Have you tested the plan for a worst case scenario	YES	20%	1
		NO	40%	2
		PARTIALLY	40%	2

Table 5Table 5: Results for Act/adjust

s/n	ACT/ADJUST		Response percentage	Response count
1	Is the information gotten from the business continuity/disaster recovery test used in the improvement of the business continuity plan?	YES	100%	3
		NO	0%	0
		PARTIALLY	0%	2
2	Do you have	YES	80%	4
	regularly updated Business Continuity arrangement that include your incident management process, notification procedures, recovery procedures and the estimated recovery time for your products, services and works?	NO	0%	0
		PARTIALLY	20%	1

VIII. DISCUSSION OF RESULTS

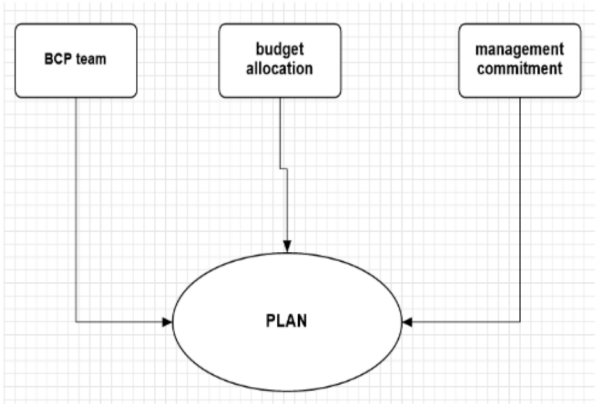

Figure 1 Diagram showing salient points derived from plan section

A. Plan

The planning section is the most important of all the sections in the PDCA circle, the planning section is the road map for achieving the business continuity and disaster recovery Plan.

From our discussions earlier, we had grouped questions that had to do with having a business continuous planning team, budget allocation for business continuity and disaster recovery and management commitment questions under the Plan section of the survey has this points are salient to having a Good business continuity and disaster recovery plan.

As shown in the figure above this three factors are paramount and should not be ignored for an effective business continuity planning.

Top management commitment: is the first and the most basic of all the points, this is where the dream is born. If the management is not convinced about having a business continuity plan, then there is not going to be a business continuity plan.

The results obtained from the survey shows that only 40 percent of managers are partially committed to having a disaster recovery while 60 percent of the various schools management are fully committed to their having disaster recovery. A partial commitment implies that there is a high

probability that those schools will not have an effective BCP/DRP. The commitment of top management will affect every single factor to having an effective BCP.

Budget allocation: a specific budget set aside for business continuity will help facilitate an effective business continuity plan. Planning, training, equipment and every other necessary to an effective Business continuity and disaster recovery mechanism require funding which if absent will make the task of having comprehensive and effective business continuity almost impossible. The fact that 80 percent of the respondents say budgets are allocated partially implies that budget funds are not enough or are not available when needed. This could hamper effective business continuity

Business continuity team: having a business continuity team or committee from all functioning sections of the institute is vital for an effective mechanism. This ensures a complete inclusion of all departments and functional units of the institute when conducting risk assessment and business impact analysis.
A total of 40 percent believes business continuity teams have representatives from every sectional section of the institution. Another 40 percent responded partially where as 20 percent indicated No.

This result implies that not every functioning unit might be involved in the planning process of the business continuity mechanism of the institutions, a neglect of a unit might lead to an important risk not been noticed or some stakeholders not been involved in the planning process. The results implies that there should be a revisiting in the forming of business continuity committee and teams in the institutions such that every functioning unit is adequately represented for an efficient team and results.

Results from the above factors show that higher educational institutes in north Cyprus have generally not consolidated an elaborate Planning process for business continuity. Managers should be fully committed, adequate funding should be made available and a team comprising of functional unit heads should be formed that should be in charge of the development of business continuity and disaster recovery of the institute

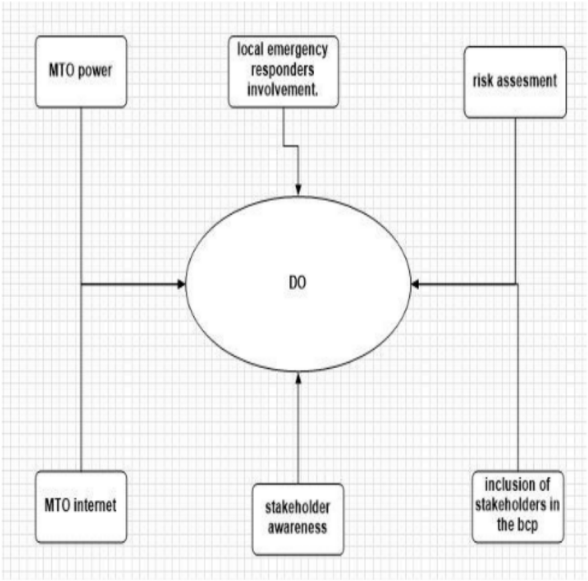

Figure 2 Showing salient points derived from the Do section.

B. Do

Questions asked under the do section of the Deming circle were centered under 6 basic points as shown in the diagram above. The implication of the results obtained is discussed as thus:
*Involving local emergency responders:*the business continuity team in the institute should involve local emergency workers like the fire service and government owned emergency agencies. Local emergency and disaster agency workers are vast with experience and expertise, collaborating with them will help in terms of disaster. 60 percent of the schools have involved local emergency responders partially while 40 percent claim to have fully involved the local emergency responders. This result implies that there is a need for the institutes to go in partnership (could be in form of a memorandum of understanding) with emergency responders that will be able to give them the necessary information on how to handle some emergency situations.
Risk assessment: Risk assessment is one of the most salient factors under this section, without a risk assessment then there is no business continuity, risk assessment is not only done for business continuity purposes alone, risk assessment help to focus on the risk that affects the workplace, the workers and the institution as a whole. A 100 percent of the respondent's claim that risk assessment for the institution is done regularly with all necessary precautions taking to mitigate the identified risk.
Stakeholder awareness: the results show that not all stake holders are aware of what to do during a disruptive situation, knowing what to do during a disaster event and doing it in time will reduce the effect of the disaster event on the business, equipment and stakeholders. Management should ensure a proper training of all stakeholders so that they are aware of what to do in case of such negative disruptive events.
*Inclusion of all stakeholders in the BCP:*the business continuity plan should cover not just

information technology (IT), equipment, or buildings but should include staffs, students. It is not uncommon for organizations to make a BC plan for just IT and exclude others. A result of 60 percent of the respondents involving all stakeholders means institutions take into account staff and students in their business continuity mechanism.

Maximum Tolerable Outage for power (MTO): there is the need for a longer MTO for power such that if there is a disruption of power from the power company the institution should be able to generate itsown power such that normal functions of the institute are not disrupted as a result of the outage of power. A shorter MTO for power implies that the institution functions that depend on power supply will be stalled in a short time after the power seizes from the power company. Our result indicates just 20 percent of the institutions have an MTO for power of over 7 days with 40 percent having their MTO to be between 1-3 days. The remaining 40 percent have an MTO to be less than a day which is not so good in case of a power disruption.

Maximum Tolerable Outage for internet: internet connectivity is very important in the present education system as almost all activities in the institution have been designed to need internet. A situation whereby internet connectivity is unavailable might affect a lot of business functions of the institute. 40 percent has an internet MTO of over 7 days 20 percent has 3-7 MTO, 20 percent of the schools has an MTO of 1-3 days while another says 6-24 hrs implies that more schools have internet backups in case of a service disruption normal functions will go on for a minimum of 7 days in 40 percent of the schools surveyed 20 percent says a minimum of a day.

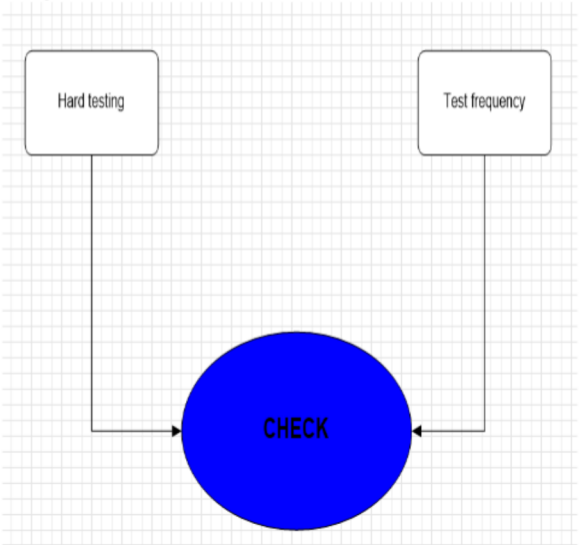

Figure 3 Salient points derived from the check section.

C. Check

Two major points were considered when accessing the check section, how frequently is the business continuity and disaster mechanism test conducted? And how hard the test was conducted.

***Test Frequency*:** 75 percent says they conduct BCP test in the institution in less than a year, 25 percent of the respondents say they conduct a test every 1 to 2 years. A frequent testing of less than a year is good as it keeps the organization up to date on how effective their business continuity mechanism is. In a very fast changing world of information technology, what might seem very appropriate could be outdated and inappropriate in a short while therefore the need for a frequent testing.

Hard Testing: testing the institutions ability to withstand disaster events for a worst case scenario is the only way the institution can know how effective their contingency plan is. A partial test might not expose weakness in the plan until tested fully. 40 percent of the respondents say they have partially conducted the plan for a worst case scenario while, another 40 percent says they have not conducted a test for a worst case scenario, only 20 percent says they have conducted a plan for a worst case scenario. Most organizations may not want to do a hard testing because it might lead to other activities being disrupted.

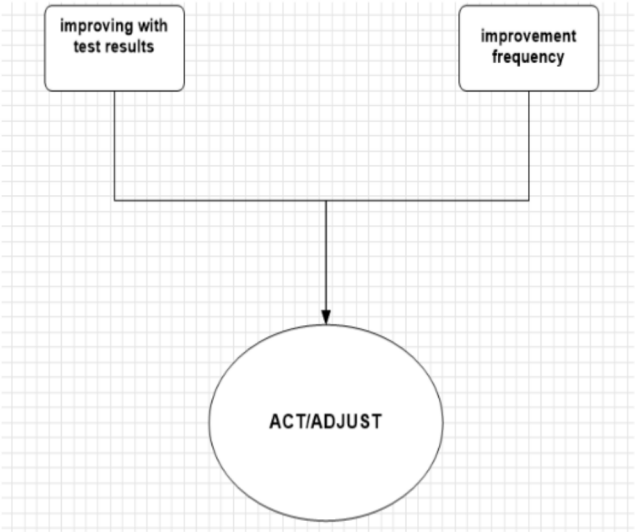

Figure 4diagram showing salient points derived from act/adjust.

D. Act/adjust

The act/adjust section is concerned with improvement of the mechanism based on the findings gotten from the tests in the check section. The two major factors highlighted in the study are:

Improvement with test results: Due to the iterative nature of business continuity, results gotten from the test should be incorporated and considered into the next planning stage of the business continuity such that weaknesses identified earlier are eliminated. A 100 percent of the respondents say they use the test results for improvement. Also 80 percent of the respondents say this identified weaknesses from the test result are used in improvement regularly.

Improvement frequency: over 80 percent of the respondents said they improve the plan regularly including all necessary changes and improve that should be made

IX. CONCLUSION

The Deming circle approach to higher education institutions business continuity and disaster recovery planning mechanism is a simple but comprehensive approach to business continuity which is suitable for evaluating higher education's business continuity mechanisms, using it to evaluate business continuity in universities in north Cyprus as shown that there are a lot of weakness and vulnerabilities in the present contingency plans available in the universities.

AUTHORS PROFILE

1. M. Dey, "Busness Contiinuity Planning Methodology-Essential For Every Business," in IEEE GCC conference and exhibition (GCC), Dubai United Arab Emirates, 2011.
2. R. Cruz and D. V. Russel, "Business Continuity Planning and Disaster Recovery Planning," in The CISSP Prep Guide Gold Edition, indianapolis, Wiley Publishing, Inc., Indianapolis, Indiana, 2003, pp. 377-408.
3. Suraj Prakash, M. Sneha , W. Abdul and S. Sundaram , "Disaster Recovery Services in the Cloud for SMEs," in IEEE Proceedings of 2012 International of Cloud Computing, Technologies, Applications & Management, 2012.
4. O. H. Alhazmi and Y. K. Malaiya, "Evaluating Disaster Recovery Plans Using the Cloud," in Reliability and Maintainability Symposium (RAMS), 2013 Proceedings - Annual, 2013.
5. O. A. Jackson, "The Impact of the 9/11 Terrorist Attacks on the US Economy. Journal of 911 studies," 2008. [Online]. Available: http://www.journalof911studies.com/volume/2008/OliviaJackson911andUS-Economy.pdf. [Accessed 3 April 2014].
6. M. E. Baird, "The Recovery Phase of Emergency Management," january 2010. [Online]. Available: http://www.vanderbilt.edu/vector/research/recoveryphase.pdf. [Accessed 4 april 2014].
7. M. Gosling and H. Andrew, " Business Continuity Statitics: Where Myth Meets Fact," 24 april 2009. [Online]. Available: http://www.continuitycentral.com/feature0660.html. [Accessed 16 april 2014].
8. R. J. Witty, "2005 BCM/DR Survey Results From Gartner, DRJ," Disaster Recovery Journal, vol. 19, no. 4, pp. 1-4, 21 march 2014.
9. T. Costello, "Business Continuity: Beyond Disaster Recovery," IEEE Computer Society Journal, vol. 14, no. 5, p. 64, 2012.
10. R. Cegiela, "Selecting Technology for Disaster Recovery," in Proceedings of the International Conference on Dependability of Computer Systems, 2006.
11. J. Smith, "Strategy Continuity Planning: The first Critical Step," Journal of Business Continuity & Emergency Planning Volume 7, vol. 7, no. 1, p. 6, 2013.
12. M. Wallace and W. Lawrence , Disaster Recovery Handbook, New york: AMACOM books, 2004.
13. E. E. Schultz, "continous monitoring: what it is, Why It Is Needed, and How to Use It," 30 june 2011. [Online]. Available: http://www.sans.org/reading-room/analysts-program/analyst-tripwire-schultz. [Accessed 12 april 2014].
14. V. Maheshwari, Rahul, Kumar Gaurav and Chandan Kumar Singh, "Business Continuity Project Planning Process for Educational institutes," International Journal of Disaster Recovery and Business Continuity, vol. 1, no. 1, pp. 1-10, 2010.
15. B. Gulachek, "Business Continuity Planning: Process Impact, and Implication," Educause Centre for Applied Research, Research Bulletin, vol. 2005, no. 13, pp. 1- 9, 21 june 2005.
16. EDUCAUSE Review Online, "Top Ten IT Issues 2011," 32 may 2011. [Online]. Available: http://www.educause.edu/ero/article/top-ten-it-issues-2011. [Accessed 8 april 2014].
17. University of Oregon's Community Service Center, "How-To Guide Partner for Disaster Resilience," Post-Disaster Recovery Planning Forum, 2007.
18. Publication by SANS institute, "Introduction to Business Continuity Planning," 2002. [Online]. Available: https://www.sans.org/reading-room/whitepapers/recovery/introduction-business-continuity-planning-559. [Accessed 28 mar 2014].

AUTHORS PROFILE

First Author Name YISA Victor Legbo.
Educational Qualification:
MSc. in Management Information System. Cyprus International University, North Cyprus
Educational Qualification:
MSc. in Management Information System. Cyprus International University, North Cyprus.
B.Eng. in electrical and computer engineering. Federal University of Technology, Minna, Niger State Nigeria.

Work experience.

- Assistant Lecturer in Department of cybersecurity science, Federal University of Technology, Minna, Niger State Nigeria. till date.
- Assistant Network Administrator in Wagitel communication Abuja.

Publication:

- The Challenges of Missing Results of E-Examination in Nigerian Universities.
  Authors: shitu kelani okunade, olawale surajudeen Adebayo, Yisa, V. Legbo and Baba Meshach. Journal of science and, technology, mathematics and education (jostmed). Volume 8(3). August 2012.
- The Simulation Of Path Control And Route Redistribution Techniques On The Integration Of WANs With Different Routing Protocols.
  Authors: S.M. Abdulhamid., V.L. Yisa., M. Baba & C.O. njoku. Journal of science and, technology, mathematics and education (jostmed). Volume 9(1). December 2012

Ongoing research work.
Bring your own device (BYOD)

Second Authors Name: BABA Meshach
Educational Qualification:
MSc. in Management Information System. Cyprus International University, North Cyprus.
B.eng. in electrical and computer engineering. Federal University of Technology, Minna, Niger State Nigeria.

Work experience.

- Assistant Lecturer in Department of cybersecurity science, Federal University of Technology, Minna, Niger State Nigeria. till date.
- Assistant Network Administrator in Wagitel communication Abuja.

Publication:

- The Challenges of Missing Results of E-Examination in Nigerian Universities.
  Authors: shitu kelani okunade, olawale surajudeen Adebayo, Yisa, V. Legbo and Baba Meshach. Journal of science and, technology, mathematics and education (jostmed). Volume 8(3). August 2012.
- The Simulation Of Path Control And Route Redistribution Techniques On The Integration Of WANs With Different Routing Protocols.
  Authors: S.M. Abdulhamid., V.L. Yisa., M. Baba & C.O. njoku. Journal of science and, technology, mathematics and education (jostmed). Volume 9(1). December 2012

Ongoing research work.
Currently researching on how big data analytics for security can be used with new national identity card to combat crime and terrorism in Nigeria.