International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Health Information Technology (HIT) Risk-Based Regulatory Framework for Informatics: Disaster Recovery and Business Continuity Plan

Eng.Adil Fagiri Babiker Fagiri[1], Dr. Hani ZakariaAsfour[2], Dr. Manal Fouad Amer[3]

MBA, Researcher at Al-Farabi College –Jeddah,

Department of Medical Microbiology and Parasitology, Faculty of Medicine, King Abdulaziz University , Researcher at Al-Farabi College –Jeddah

Lecturer, Nursing Administration Department , Al-Farabi College for Nursing and Dentistry, Jeddah, Saudi Arabia Faculty of Nursing, Cairo-University, Egypt.

Abstract: ***Business continuity and disaster recovery plan is the act of proactively working out a way to prevent, if possible, and manage the consequences of a disaster, limiting it to the extent that a business can afford. This research aims at identifying the reality of the usage of business continuity and disaster recovery plan of the information technology department at Al-Farabi College. A modified model for achieving the research purpose was used; this model is a modified mixture between the suggested steps/components in disaster recovery and business continuity. Comprehensive survey technique was used and two questionnaires were distributed to all head of sections of information technology department .Findings showed that (%54.8) of college departments faced a disaster in their computer systems and most of disasters were caused by infrastructure threats, and the software was the most affected part. Data compiled from respondents that (76.3%) information technology department had the plan, but actually they did not follow all the necessary of its procedures and components. Also, results showed that plan development procedures were the weakest component. The researchers recommended the information technology department heads to give more concern to the different components of the plan based on research findings.***

Keywords: Management information system, Business Continuity, Disaster Recovery, Informatics, Health information technology.

1. Introduction

Business continuity and disaster recovery refers to an organization's ability to recover from a disaster and/or unexpected event and resume operations, which has highly developed speedily over the years, as it is forms now a crucial component for conducting business. The Act is telling responders and planners that businesses require having continuity planning measures in place in order to survive and continue to thrive whilst working towards custody the unpleasant incident as minimal as possible. (10)

Organizations often have a plan in place that outlines how a recovery will be accomplished. The key to successful disaster recovery is to have a plan well before disaster ever strikes. Business continuity planning (BCP, also called business continuity and resiliency planning BCRP) identifies an organization's exposure to internal and external threats and synthesizes hard and soft possessions to provide valuable prevention and recovery for the organization, while maintaining competitive advantage and assessment system integrity. (2)

Business Continuity and Disaster Recoveryis stand for processes that help organizations prepare for disruptive events—whether an event might be a hurricane or simply a power outage caused by a backhoe in the parking lot. Management's involvement in this process can range from overseeing the plan, to providing input and support, to put the plan into action during an emergency. Business continuity and disaster recovery planning supports this requirement by establishing through plans, procedures, and technical measures that can enable a system to be recovered quickly and effectively following a service disruption or disaster. Interim measures may include the relocation of information technology systems and operations to an alternate site, the recovery of information technology functions using alternate equipment's, or the performance of information technology functions using manual methods

According to David Bird, (8), within the current century there is increased dependence for businesses on information technology, reliance on business-critical information and importance of protecting irreplaceable data. Most companies are relying on their computer systems as critical infrastructure in their business. Majority of companies are aware that they need to back up their data to limit information loss and to aid data recovery. The largest part of companies does not have a disaster recovery plan.

Business continuity and disaster recovery planning are not new concepts to business, but the act of consciously assessing and planning for potential problems certainly has been underscored by disastrous events in the past decade including earthquakes, tsunamis, hurricanes, typhoons, and terrorist attacks. Information technology heads sections is needed to plan for potential disasters that will impact their ability to continue operations and earn income. Without a plan to recover from any disaster or event, no matter how large or small, many Information technology heads sections fail. The statistics speak for themselves. The odds are between 40% and 50% that a company will fail after a fire or significant data loss, and that only 6% of Information technology heads sections survive long-term after a major incident. (62).

Disaster recovery planning devises plans for the restoration of computing and communications services after they have been disrupted by an event such as an earthquake, flood, or terrorist attack. Disaster recovery plans focus primarily on the technical issues involved in keeping systems up and running, such as which files to back up and the maintenance of backup computer systems or disaster recovery services (4&3).

Health information technology (HIT)(9) is "the application of information processing involving both computer hardware and software that deals with the storage, retrieval, sharing, and use of health care information, data, and knowledge for communication and decision making".1 Technology is a broad concept that deals with a species' usage and knowledge of tools and crafts, and how it affects a species' ability to control and adapt to its environment. However, a strict definition is elusive; "technology" can refer to material objects of use to humanity, such as machines, hardware or utensils, but can also encompass broader themes, including systems, methods of organization, and techniques. For HIT, technology represents computers and communications attributes that can be networked to build systems for moving health information. Informatics is yet another integral aspect of HIT.

Informatics refers to the science of information, the practice of information processing, and the engineering of information systems. Informatics underlies the academic investigation and practitioner application of computing and communications technology to healthcare, health education, and biomedical research. Health informatics refers to the intersection of information science, computer science, and health care. Health informatics describes the use and sharing of information within the healthcare industry with contributions from computer science, mathematics, and psychology. It deals with the resources, devices, and methods required for optimizing the acquisition, storage, retrieval, and use of information in health and biomedicine. Health informatics tools include not only computers but also clinical guidelines, formal medical terminologies, and information and communication systems. Medical informatics, nursing informatics, public health informatics, and pharmacy informatics are sub disciplines that inform health informatics from different disciplinary perspectives. The processes and people of concern or study are the main variables.

2. Method

The research aims to identify the reality of the usage of Business Continuity and Disaster Recovery plan in information technology department at Al-Farabi College. The researcher used a modified model for achieving the research purpose; this model is a modified mixture between the suggested steps/components in Business Continuity and Disaster Recovery models. The questionnaire was used to collect the information, and it was designed like a 1-10 scale to determine to what extent are business continuity and disaster recovery plan components are used in information technology department at Al-Farabi College.

2.1 Objectives of the Research

The research aims at achieving the following objectives:

1) To identify the reality of the usage of business continuity and disaster recovery planning in Al-Farabi Collegelisted department.
2) To identify the types of disasters and disruptions faced in Al-Farabi Collegelisted department.
3) To identify the most effective component of business continuity and disaster recovery plan in Al-Farabi College listed department.
4) To extract a modified model for business continuity and disaster recovery plan from previous models.
5) To present suggestions to information technology departments that may help and support them in their business continuity and disaster recovery planning.

2.2 Hypothesis

The study examines the following hypothesis:

The first hypothesis:
There is a significant difference in the level of existence of the seven components of business continuity and disaster recovery between the responded department (Project initiation techniques, Risk Assessment, Business impact analysis, Mitigation strategy, Plan development, Testing auditing and maintaining, Training).

The second hypothesis:
There is a correlation between the level of existence of business continuity and disasterrecovery and the seven components.

The third hypothesis: There is no significant difference among respondentsregarding the application of business continuity and disaster recovery plan attributed to thefollowing variables:

- Job Title.
- Qualification.
- Experience.
- Age.
- Company size.
- Staff number

2.3 Research Variables

Based on the above hypothesis we can say that the study has one dependent variable,which is business continuity and disaster recovery plan. This variable is followed by anumber of independent variables that measure the extent to which the independent variableaffect the dependent one to verify the validity of the proposed hypothesis. The independentvariables of the study are:

1. Job Title
2. Qualification.
3. Experience.
4. Age.
5. Company size.
6. Number of information technology staff.
7. Project initiation techniques.
8. Risk assessment.
9. Business impact analysis.

10. Mitigation strategy.
11. Plan development.
12. Testing, auditing and maintaining.
13. Training.

2.4 Importance of Research

This research has its own significances on both the academic and practical levels:
This study reflects the reality of business continuity and disaster recoverysystem followed in The Al-Farabi. College department, and the extent of success andeffectiveness of this program.This study will contribute in formulating a clear vision to evaluate businesscontinuity and disaster recovery plans, which will benefit all of informationtechnology specialists in the studied department

2.5 Scope of Study

This research studies the entire listed department in Al-Farabi Collegesecurities exchange.The researcher chose the listed department to be studied because of the widedependent of those departments on information technology, and the ability of those departments to apply and fund business continuity and disaster recovery plans.

3. Study Methods and Data Collection

Analytical descriptive techniques were used to sustain quantitative and qualitative measurement and analysis. The researcher utilized different tools to collect primary and secondary data as follows:

Primary data: to introduce the theoretical literature of the subject, the researcher used the following data sources: Books, Periodicals, published papers, and articles in English about business continuity and disaster recovery planning. Web sites and electronic versions.

Secondary data: In order to analyze the qualitative and quantitative data of the study, questionnaire was used as a tool for collecting primary data. The questionnaire consists of the following parts
Part One: considers the personal characteristics of the respondents.
Part two: considers company profile and disaster cases.
Part three: considers components of business continuity and disaster recovery plan.

The third part consists of a set of forty six questions selected to measure the level ofexistence of the business continuity and disaster recovery components. Researchers were requested to fill the questionnaire through writing a number that ranges from 1 to 10 for each answer. Researchers were provided clear instructions to fill the questionnaire and it was made clear to them that the more the answers are close to 10 the more they agree with the statement to be measured. Every question has 10 alternative answers according to scale which ranges from 1 to 10, 1 means absolute disagreement with the statement and 10 means absolute agreement.

Questionnaires were distributed to all heads of sections of informationtechnology department and then the input will be analyzed using the SPSS.

4. Research Population

Survey was conducted for all of information technology heads of sections or their deputies according to the organizational structure. A comprehensive survey was used in this study.

The researchers included all those section of information technology department in collecting the needed data.
Two questionnaire were distributed to every head, 62 questionnaire from 31 answers were valid which shape about (81.6%) from the sample. On the other hand, questionnaires were distributed though email.

4.1 Validity and reliability of the questionnaire

The measurement has been applied on 30 answers which were randomly selected as pilot study aiming at checking the validity and reliability of the questionnaire. The pilot sample has been distributed on the 20th of April 2014 and was collected in 2 weeks, and the all of these participants were involved in the final analysis.

5. Results

Type of data

In small sample studies usually conducting KolomogrovSimrnov Test is necessary to examine whether the data is parametric or non-parametric. The distribution for each component is not normally distributed based on Kolmogorov- Smirnov test, since the P-value (sig.) is smaller than the level of significance <= 0.05 .Sodata is non-parametric. See table (1).

Table 1: Kolmogorov-Smirnov test value

Field	Kolmogorov-Smirnov test value	P-Value (Sig.)
Project Initiation	0.265	0.000*
Risk Assessment	0.258	0.000*
Business Impact Analysis	0.204	0.000*
Mitigation Strategy Development	0.233	0.000*
Business Continuity/Disaster Recovery Plan Development	0.215	0.000*
Business Continuity/Disaster Recovery Plan Testing	0.321	0.000*
Business Continuity/Disaster Recovery Plan Auditing	0.233	0.000*
Business Continuity/Disaster Recovery Plan Maintenance	0.207	0.000*
Business Continuity/Disaster Recovery Plan Testing, Auditing, and Maintenance	0.159	0.001*
Business Continuity/Disaster Recovery Training	0.305	0.000*
All the seven components	0.155	0.001*

* Correlation is significant at the 0.05 level

Analyzing and discussing the dimension of the questionnaire Sign test is used to determine if the mean is significantly different from a hypothesized value 6. If the P-value (Sig.) is smaller than the level of significance, <= 0.05, then the mean is significantly different from a hypothesized value 6. The sign of

6. Business Continuity/Disaster Recovery Plan Development

Table (2) revealed that all the mean values of paragraphs related to Business Continuity/Disaster Recovery Plan Development dimension more than 6 and P-value more than .05, which means that most Plan Development procedures were well applied in the business continuity and disaster recovery planning in information technology departments of the targeted department, for example Plan Development of targeted department had stated the risks, the vulnerabilities, and the potential impact to each of the mission-critical business functions (67.41%), The plan development defined the initial actions taken once a system disruption has been detected(66.38%), plan development stated mitigation strategies, methods of applying, people, resources, and tasks needed to complete these activities(68.79%). At overall the total score of the dimension "Business Continuity/Disaster Recovery Plan Development" was (67.28%) and P-value was (0.081). It means that the majority of the targeted department had written the most important procedures to handle any disaster occurred in their business continuity and disaster recovery plan, where the remaining had weaknesses in writing their procedures. I was concluded that 67.28% of the business continuity and disaster recovery plan components were written in department' plans, while the remaining of the components did not list yet, which means that there is a weakness to some extent in writing the business continuity and disaster recovery plans in the targeted department. While the P-Value more than 5%, it reflected that the targeted department did not agree to a unified and similar answer in developing their plan. This was due to the fact that not all of department had written their plan and not all of thedepartment had such plans, which reflect a weakness in writing the plans in some of department. The results of this dimension come on line with other previous researchers:

1) (6): The result of this study demonstrated that (50%) of respondents have fully integrated or comprehensive business continuity plans.
2) (7): This paper suggested steps to develop successful disaster recovery plans, which included develop and implement the plan.
3) (5): This paper suggested a methodology to develop suitable business continuity and disaster recovery plan, which included Plan development.

Table 2: The mean and test value for "Business Continuity/Disaster Recovery Plan Development"

No	Paragraph	Mean	Proportional Mean%	Test value	PP-value(Sig.)	Rank
1	In plan development you take mitigationstrategies and identify methods for implementingthose strategies, people, resources, and tasksneeded to complete these activities.	6.88	68.79	2.24	0.013*	1
2	In plan development you stated the risks, the vulnerabilities, and the potential impact to each of the mission-critical business functions. For each of these, there should be associated mitigation strategies	6.74	67.41	1.43	0.077	2
3	In plan development you define communications plan to control the communication while a disaster occurred.	6.66	66.55	1.27	0.102	3
4	In plan development you define the initial actions taken once a system disruption or emergency has been detected.	6.64	66.38	1.27	0.102	4
	Business Continuity/Disaster Recovery Plan Development	6.73	67.28	1.4	0.081	

7. Business Continuity / Disaster Recovery Plan testing

Table (3) revealed that all the mean values of paragraphs related to Business Continuity/Disaster Recovery Plan Testing dimension more than 6 and P-value less than .05, which means that most Plan Testing procedures were well applied in the business continuity and disaster recovery planning in information technology departments of the targeted department, for example Plan Testing of targeted department had tested their plans in a regular basis (80.69%), plan at least tested annually (80.17%), tests gave a complete data about the weaknesses of the plan(80.17%). At overall the total score of the dimension "Business Continuity/Disaster Recovery Plan Testing" was (80.78%) and P-value was (0.0). It means that the majority of the targeted department had accurate, rich, and comprehensive procedures in testing their plans. It was concluded that 80.78% of business continuity and disaster recovery plan testing procedures and objectives were implemented and followed up in the targeted department' plans. This is due to the fact that most of the leaders have experience in such topic, and they know that the technology is rapidly and continuously changed, so testing from period to period is obligated to test the plan validity and availability. Moreover no risk assessment and business impact analysis is complete, so a real test can discover the weaknesses in the previous stages which made inadvertently.

Table 3: The mean and test value for "Business Continuity/Disaster Recovery Plan Testing"

No	Paragraph	*Mean*	*Proportional Mean%*	*Test value*	*PP-value(Sig.)*
1	In plan development you stated the risks, the vulnerabilities, and the potential impact to each of the mission-critical business functions. For each of these, there should be associated mitigation strategies	8.07	80.69	5.22	0.000*
2	In plan development you define communications plan to control the communication while a disaster occurred.	8.02	80.17	4.67	0.000*
3	In plan development you define the initial actions taken once a system disruption or emergency has been detected.	8.21	82.07	5.77	0.000*
4	Plan testing identifies gaps or weaknesses in the plan.	8.02	80.17	5.41	0.000*
	Business Continuity/Disaster Recovery Plan Development	8.08	80.78	5.12	0.000*

8. Discussion

Conclusions

In light of the findings that were presented in the last chapter, one can say that the business continuity and disaster recovery plans were found in the information technology departments of Al-Farabi College -Jeddah. This is a high risky situation, because as revealed from the analysis in the last chapter, the majority of the Information technology heads sections faced a disaster in their computer systems, and if there is any weakness in the plan, the plan may go in vain.

Data compiled from respondents indicates that there were proper background education that the information technology managers of the targeted Information technology heads sections have, the majority of research respondents were working as decision makers in their departments, which reflects their level of effectiveness in their jobs, the majority of research respondents were specialized in computer; this properly reflects their educational background is related to their field of work, which may help them and facilitate their duties, (67.8%) of the respondents are having not less than ten years of experience This is good that respondents have enough experience years; they will help to get more precise practice and results according to what they have practiced during their long professional live.

It was concluded that most Al-Farabi College -Jeddah Information technology heads sections consider as large department, so it has to apply business continuity and disaster recovery planning in their businesses, Information technology heads sections diverse in introducing information technology services in targeted department, Information technology heads sections depends mainly on information technology services, but actually there were also the lack of spatiality inside information technology departments. Information technology heads sectionswere diverse in the size and type of informationtechnology services introduced to department, but 58.1% less than 3 workers actually indicates weaknesses in the human resource requirements in information technology department in the targeted department.
Data compiled also revealed that (54.8%) of respondents' Information technology heads sections had a disaster threat during its life, which reflects the importance of planning for business continuity and disaster recovery planning. (83.3%) are caused by infrastructure threats. This reflects that most of disasters were made suddenly, such as breakdown in hardware, or electricity interruptions effects. And most of disaster stroked software.

It was revealed that most Information technology heads sections had the plan, but actually they did not follow all of necessary procedures and components in the plan, for example: most of project initiation techniques were found in the plans but not all them, Risk assessment, business impact analysis, mitigation strategies development procedures are applied to a high extent in the targeted Information technology heads sections but not all of proposed procedures.

(76.3%) of the project initiation techniques were found, this due to the high awareness of the significance of business continuity and disaster recovery planning among information technology managers, and management, where they are aware of the consequences in case of weak business continuity and disaster recovery planning. Moreover most of the leaders are specialized or they have experience in business continuity and disaster recovery planning, which mean that most of them have good knowledge with basics of business continuity and disaster recovery planning. This is logical and reasonable because we are in 2009, and this topic is considered as one of the most information technology managers' modern priorities, and all of specialists are considered to be in line with the newest technology management.

(75.86%) of the Risk Assessment procedures were found, this is due to the serious steps followed in assessment, in order to avoid the consequences ofweak analysis and assessment. This happens because most of the leaders have experience in the field of business continuity and disaster recovery, as they are in line with the modern technology, and they are responsible for any emergency cases that may happen.

(74.05%) of the Business Impact Analysis procedures were found. It means that the majority of the targeted Information technology heads sections are practicing a good procedures and nearly comprehensive analysis in business impact analysis. This is duo to the awareness of the impact of this analysis on the company, and this is done without any extra-costs over the department.

(82.81%) of the Mitigation Strategies were found, It means that the majority of the targeted Information technology heads sections had solutions to mitigate the expected disaster, where the mitigation strategies cover critical data, critical systems and infrastructure. This occurred because most of these steps and procedures are mainly technical procedures, where the information technology teams in the targeted Information technology heads sections had good skills and experience in such field.

Moreover most of Information technology heads sectionscan provide the required materials and equipment's to the team, because of the low cost relatively with cost of consequences in case of disaster attract consequences.

I was concluded that 67.28% of the business continuity and disaster recovery plan components were written in department' plans, while the remaining of the components did not list yet, which means that there is a weakness to some extent in writing the business continuity and disaster recovery plans in the targeted department. While the P-Value more than 5%, it reflected that the targeted Information technology heads sections did not agree to a unified and similar answer in developing their plan. This was due to the fact that not all of Information technology heads sections had written their plan and not all of the Information technology heads sections had such plans, whichreflect a weakness in writing the plans in some of department.

It was concluded that plan testing, auditing, and maintaining procedures applied in the targeted Information technology heads sections were good, but not enough to keep the plan valuable and effective.

This is due to the high importance of ensuring the readiness of the plan, without this all of the previous stages and activities may be wasted. So leaders worked strongly for this topic. It was concluded that most Information technology heads sections were interested in implementing training to their employees, this is due to the high importance of this topic, and the rapid change in the related used technologies. Moreover the cost of training is less than the risk that the company can afford in case of disaster. Analysis of the questionnaire showed that plan development procedures are the weakest component of the plans developed in the targeted department.

Testing, auditing, maintaining, and training procedures were followed, but Information technology heads sections need more enhancements to the implemented procedures.

It was concluded that the most existed component in the plan was the mitigation strategies. This is because most of Information technology heads sections have proper and adequate actions to handle with potential disasters, where the implementation of these strategies is easy and mainly technical issue. Moreover most of the leaders and information technology teams are well trained, and there are a training scenarios and handbooks available in the internet. While the least existed component was plan development. This is because not all information technology leaders are organized, and they depend mainly on their minds memory, or they were not strongly requested to write a plan to mitigate such cases.

In the second hypothesis, it was assumed that there is a correlation between level of existence of Business Continuity and Disaster Recovery and the seven components of the plan, we found out that thesig. is .000 < .05 which clearly indicates that the relationship between the existence of the plan and the seven components of the plan. It was also found out that the correlation is (.721**) which evidently indicates that the correlation is positive.

This means that: The more existence of the project initiation techniques, better accurate and deep risk assessment, better accurate and deep business impact analysis, existence of mitigation strategies, comprehensive Business Continuity / Disaster Recovery Plan Development, accurate and deep plan testing auditing maintenance, and training the more existence of good and effective business continuity and disaster recovery plan.

It was also concluded from the high correlation of most components of the plan, that the availability of each component in the plan is essential and mandatory, and without its existence the plan will be incomplete and weak.
This is logic and reasonable, because the plan without one of these components it may be useless, where each component shapes a cornerstone in the process of planning, and weaknesses in the implementation procedures of one of

these components may deconstruct all of the efforts done in the others components.

It was concluded also, that plan testing, auditing and maintaining is the most important component of the plan, then risk assessment, then business impact analysis.
In the Third hypothesis, it was concluded that:

1) The respondents' qualification, job title, experience, age had no effect on the application of Business Continuity and Disaster Recovery.
2) It was concluded that the respondents' Specialization had an effect on the application of Business Continuity and Disaster Recovery.

9. Recommendations

- In light of the aforementioned results the researcher recommends the following, wishing from I.T. management, researchers to take them into account and put them into action:
- Researcher advised Information technology heads sections to give more concern to Project Initiation techniques.
- Researcher advised Information technology heads sections to give more concern to Risk Assessment.
- Researcher advised Information technology heads sections to give more concern to Business Impact Analysis.
- Researcher advised Information technology heads sections to enhance their practicing toward mitigation strategy of
- Web Sites by taking in account backing up and storing Web Sites through Load balancing strategies to ensure web sites have high availability.
- Researcher advised Information technology heads sections to spend more efforts in amending the Plan Development.
- Researcher advised Information technology heads sections to enhance their practicing toward Plan Maintenance.
- Researcher advised Information technology heads sections to enhance their practicing toward Plan Auditing.
- Researcher advised Information technology heads sections to adopt business continuity and disaster recovery plans according to the suggested model in this study.
- Al-Farabi College -Jeddah authority is advised to prepare a law to mandate Al-Farabi College -Jeddah to prepare their own business continuity and disaster recovery plans according to such this model suggested in this study.
- Researcher advised Information technology heads sections to train their employees to collaborate with researchers, and to enhance scientifically research culture between their employees.
- Al-Farabi College -Jeddah library manager is advised to enrich the library with references related to the topic of research.

10. Future Work

Researchers are advised to apply this field of research on others sectors such as: governmental ministries, and higher education institutes.

References

[1] Brailer, D., & Thompson, T. (2004). Health IT strategic framework. Washington, DC: Department of Health and Human Services. http://ushik.org/ViewItemDetails?system=ps&itemKey=88747000
[2] Elliott, D., E. Swartz, et al. (1999). "Just Waiting for the Next Bang: Business Continuity
[3] Greer Gregg,(2003), ―Higher Education Business Continuity Survey ,Master Thesis, Baylor University, Waco, Texas, USA.
[4] Laudon K. and J. laudon, (2006), Management Information Systems: Managing the Digital Firm, 9/e.,Pearson Prentice Hall , ISBN 9780136078463].
[5] MohHeng, Goh,(1996), "Developing asuitable business continuity planning odology",Information Management & Computer Security. Bradford: 1996. Vol. 4, Iss. 2;
[6] Paton Douglas, (1999), "Disaster business continuity: promoting staff capability", Disaster Prevention and Management. Bradford: 1999. Vol. 8, Iss. 2. Poilt, D., and Hungler, B., 1985. "Essentials of nursing research; Methods and applications", J. B. Lippincott company. Pitt; Michael and Sonia Goyal,(2004), "Business continuity planning as a facilities management tool",Facilities; 2004; 22, 3/4; ABI/INFORM Global.
[7] Wong Bo K; Monaco, John A; andSellaro, C Louise, (1994)., "Disaster recovery planning:
[8] Virginia Cerulloa& Michael J. Cerullo , (2004), Business Continuity Planning: A Comprehensive Approach , Journal of Information Systems Management Vol 21 (3), PP.1
[9] http://en.wikipedia.org/wiki/Health_information_technology
[10] Mitchell,J,(2013).International Business Continuity Portal. Business continuity and disaster recovery: big tent, or separate umbrellas?, http://www.continuitycentral.com/feature1105.html