The Islamic University-Gaza
Higher Education Deanship
Faculty of Commerce
Master of Business Administration Department

Evaluating Business continuity and Disaster recovery planning in information technology departments in Palestinian listed companies

Submitted By
Mohammed Enshasy

Supervised By

Prof. Majed El-Fara

Submitted in Partial Fulfillment of the Requirement for the Degree of MBA

November, 2009

Dedication

To those whose kindness, patience and support were the candles that enlightened my way towards success; my Father and Mother.

To my beloved wife who saved no efforts in encouraging and supporting me during my journey toward success, and to here extended family.

To my brothers and my sisters who spiritually supported me.

ACKNOWLEDGMENT

My gratitude is deeply paid to my advisor, Professor Majed El-Farra for his generosity, guidance and advice. Of course, I would not forget Prof. Yousif Ashour and Dr. Rushdy Wady for accepting to discuss this study.

I am also grateful to Dr. Samir Safi for help with statistical analyses on my data, follow up and revision of the empirical part of the research.

Special thanks are due to the Islamic University and its staff for all the facilities, help and advice they offered.

Special thanks are due to KYTC Principal Dr. Ghassan Abu-Orf and his staff for their morale and spiritual support.

Not forgetting to thank my dear colleagues and friends for their encouragement and support especially Mr. Ahmad Alsufi for his fruitful efforts during this study.

Table of Contents:

List of Tables

List of Figures

List of Appendices

الملخص

"تقيم التخطيط لاستمرار العمل والاستعادة الكوارث في أقسام تكنولوجيا المعلومات في الشركات المدرجة في سوق فلسطين للأوراق المالية"

هدفت هذه الدراسة إلي التعرف على واقع استخدام التخطيط لاستمرار العمل والاستعادة من الكوارث في أقسام تكنولوجيـا المعلومـات في الشركات المدرجة في سوق فلسطين للأوراق المالية، وكذلك إلى التعرف على أنواع الكوارث التي أصابت تلك الشركات.

ولقد استنبط الباحث نموذجا جديداً لتحقيق هدف الدراسة، وكان هذا النموذج عبارة عن خليط بين نموذج كل مـن مؤسـسة معلومـات الاستعادة من الكوارث العالمية ومؤسسة استمرار العمل.

وطبقت الرسالة على الشركات المدرجة في سوق فلسطين للأوراق المالية في الفترة الزمنية ما بين الأول من يناير 2008 إلي الثلاثين من يونيو 2009.

ولقد استخدم الاستبيان كأداة لجمع البيانات، وصممت إجاباته لتكون ما بين 1- 10، لتبيان إلي أي درجة تطبق مكونات خطـة اسـتمرار العمل والاستعادة من الكوارث في الشركات المدرجة.

ولقد تم استخدام أسلوب المسح الشامل، وتم توزيع الاستبانه على مدراء أقسام تكنولوجيا المعلومات في الشركات المدرجة وعددها 38 شركة بواقع استبانتين لكل شركة، أو رؤساء الأقسام، أو من ينوب عنهم، تبعاً للهيكل التنظيمي للشركات.

ولقدت أظهرت نتائج الدراسة أن 54.8% من الشركات سبق لها وأن واجهت حدثاً كارثياً في مجال تكنولوجيا المعلومات، ومعظـم هـذه الكوارث كانت بسبب أعطال في البنية التحتية لنظم المعلومات، وكانت البرامج أكثر من تأثر بده الكوارث.

ولقد أظهرت نتائج البحث أيضاً أن خطط استمرار العمل والاستعادة من الكوارث في هذه الشركات لا تتبع الخطوات الـضرورية والكاملـة للخطة، فعلى سبيل المثال فإن (76.3%) من تقنيات المشروع موجودة في الخطة ولكن ليس كلها. كذلك فإنه يمكن القول بأنـه تم تطبيـق خطوات تقدير الأخطار، وتحليل أثر الأخطار، واستراتيجيات مواجهة الكوارث بدرجة عالية في الشركات المستهدفة، ولكن لم يكن التطبيـق كاملاً كالنموذج المقترح.

كما أظهرت نتائج البحث أن خطوات تطوير وصياغة الخطة كانت المكون الأضعف في الخطط، وكانت استراتجيات مواجهة الكوارث هـي المكون الأكثر وجوداً في الخطط، وأن كلاً من خطوات الاختبار والتدقيق والتعديل والتدريب كانت متبعة ولكن ليس بشكل متكامل.

ولقد نصح الباحث الشركات بزيادة اهتمامها بمكونات الخطة المختلفة.

Abstract

"Evaluating Business continuity and Disaster recovery planning in information technology departments in Palestinian listed companies"

This study aims at identifying the reality of the usage of business continuity and disaster recovery planning in information technology departments of Palestinian listed companies, and identifying the types of disasters and disruptions faced Palestinian listed companies.

The researcher used a modified model for achieving the research purpose, this model is a modified mixture between the suggested steps/components in DRII and BCI models.

This research studied all the listed companies in Palestine Securities Exchange, for the period from January, 1st 2008 to June, 30th 2009.

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 the listed companies.

Comprehensive survey technique was used, and two questionnaires were distributed to all managers or head of sections of information technology departments in 38 targeted companies, according to the organizational structure of companies.

Analysis of the questionnaire showed that (%54.8) of the companies 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 through questionnaire revealed that (76.3%) companies had the plan, but actually they did not follow all the necessary procedures and components of the plan, for example: most of project initiation techniques were found in the plans but not all, risk assessment, business impact analysis, and mitigation strategies development procedures were applied to a high extent in the targeted companies but not all of proposed procedures.

Analysis of the questionnaire also showed that plan development procedures were the weakest component of the plans developed in the targeted companies. Where testing, auditing, maintaining, and training procedures were followed, but companies need more enhancements to the implemented procedures. And finally the most existed component in the plan was the mitigation strategies.

The researcher recommended companies to give more concern to the different components of the plan.

Chapter One:
An Introduction

1. An Introduction

1.1. Introduction

Information technology industry has advanced rapidly over the years, so that it forms now a vital component for conducting business (Botha and Solms,2004).

These days, where individuals and corporations have become increasingly reliant upon information technology , to the extent that it is difficult to find a corner of a company that technology does not touch, and the majority of organizations cannot operate without computer systems (Barbara, 2006).

As technology continues to become more integral to corporate operations at every level of the organization, the job of information technology has expanded to become almost all-encompassing. As businesses increasingly rely on data, information and technology, new threats are constantly emerging that affect all corporations and many companies have experienced or witnessed the devastation that occurs when an information technology disaster strikes (Barbara, 2006).

As information technology systems evolve, they also need to be protected against today's considerable amount of threats to the information they process, transmit and store. So any failure or disaster in information technology system could have a serious consequences for a company (Botha and Solms,2004), and as a result of depending the majority of those companies on these systems, no company can afford to ignore the need for business continuity and disaster recovery planning regardless of the company size, revenues, or number of staff, and the need to plan for potential disruptions to technology services has increased exponentially and business continuity and disaster recovery planning has become imperative (Snedaker, 2007).

In the late 1990s, Business continuity planning came to the forefront as businesses tried to assess the likelihood of business systems failure on or after January 1, 2000 (the now infamous “Y2K” issue), Business continuity planning is a methodology used to create and validate a plan for maintaining continuous business operations before, during, and after disasters and disruptive events. Business continuity planning has to work on managing the operational elements that allow a business to function normally in order to generate

revenues, and also to keep the company running, regardless of the potential risk, threat, or cause of an outage (Snedaker, 2007).

The business continuity plan is developed to prevent interruptions to normal business. If these events cannot be prevented, the goals of the plan are to minimize the outage and reduce the potential damage that such disruptions might cost the organization. Therefore, the business continuity planning should also be designed to help minimize the cost associated with the disruptive events and mitigate the risks associated with these disruptive events (Gregg, 2007). Business continuity planning involves developing a collection of procedures for the various business units that will ensure the continuance of critical business processes while the data centre is recovering from the disaster (Wilson, 2000).

1.2. Problem Statement

No one can deny the role of information technology in facilitating company's functions. This role entered the depth of every company's core and extrinsic function, to the extent that information technology has become a vital part of conducting business in our advanced technologically environment. Palestinian companies are considered as one of those companies which implement information technology in a lot of its functional fields, and depend basically on information technology to achieve its missions.

And because of the threatens caused by several disruptive and disaster to the information technology systems, and the unstable environment caused by occupation and other internal factors, it became an obligation to information technology managers -not optional- in those companies to protect their information technology systems against any emergent disaster, to keep their business running despite of the existence of threatens, especially after the occurrence of several events such as the Israeli attack on Palestinian electricity company, the Israeli bulldozing of Paltel infrastructure in north of Gaza, the attract of several viruses which interrupt and disable the use of computers, and the burning of Islamic university, this protection can be done by developing business continuity and disaster recovery plan.

So this study will investigate reality of usage of business continuity and disaster recovery planning in information technology departments in the listed companies in Palestine securities exchange, and its success and effectiveness.

1.3. 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 Palestinian listed companies.
2. To identify the types of disasters and disruptions faced in Palestinian listed companies.
3. To identify the most effective component of business continuity and disaster recovery plan in Palestinian listed companies.
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.

1.4. 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 companies (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 disaster recovery and the seven components.

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

- Job Title.
- Qualification.
- Experience.

- Age.
- Company size.
- Number of information technology staff.

1.5. 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. These variable is followed by a number of independent variables that measure the extent to which the independent variable affect the dependent one to verify the validity of the proposed hypothesis. The independent variables 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.

1.6. 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 recovery system followed in the Palestinian companies, and the extent of success and effectiveness of this program.
- This study will contribute in formulating a clear vision to evaluate business continuity and disaster recovery plans, which will benefit all of information technology specialists in the studied companies.

1.7. Scope of Study

This research studies all the listed companies in Palestine securities exchange.

The researcher chose the listed companies to be studied because of the wide dependant of those companies on information technology, and the ability of those companies to apply and fund business continuity and disaster recovery plans.

1.8. Research Structure

Chapter one : An Introduction.

Chapter two : Business continuity and Disaster recovery.

Chapter third : Overview of Palestine Securities Exchange Listed Companies, and Information Technology.

Chapter fourth: Previous Studies

Chapter Fifth : Research Methodology

Chapter sixth : Empirical Framework Hypothesis Testing & Discussion

Chapter seventh: Findings and Recommendations

Chapter Two:
Business continuity and disaster recovery planning

Preface:

This chapter will review the definition of business continuity and disaster recovery planning, its evolution, and impact of Year 2000 problem, objectives, importance, and major benefits and inhibitors.

Also this chapter will address the process of preparing a business continuity and disaster recovery which will be considered as the study model. The detailed elements of Business Continuity and Disaster Recovery plan will be reviewed and step-by-step plan preparation and activation guidance will be provided.

The basic steps in any Business Continuity and Disaster Recovery plan include:

- Project Initiation
- Risk Assessment
- Business Impact Analysis
- Mitigation Strategy Development
- Plan Development
- Plan Testing, Auditing, and Maintenance
- Business Continuity and Disaster Recovery Training

2.1 Introduction to business continuity and disaster recovery planning

Today, business entities exist in a highly competitive world. They are constantly innovating to meet their business objectives of providing essential and unique services to their customers, and organizations rely more than ever on technology, because technology advances have enabled them to achieve their varied strategies (Ramesh, 2002).

So information systems are a vital element in most today's business processes, and because information technology resources are so essential to an organization's success, it is critical that the services provided by information technology systems are able to operate effectively without excessive interruption (Lennon, 2002), and as companies increasingly rely on digital systems for their revenue and operations, they need to take additional steps to ensure that their systems and applications are always available (Laudon and others, 2006).

And yet, on account of business interruption, the threats of disaster are not extinct, they have also evolved along with the technology. Business continuity and disaster recovery planning 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 (Ramesh, 2002).

And in the face of increasingly realistic threats from natural disasters, terrorism, cyber attacks, and technical disaster, organizations have placed increasing emphasis on assuring the technology that drives their businesses will run without interruption (Ramesh, 2002; Williamson, 2007).

Firms such as those in the airline and financial services industries with critical applications requiring online transaction processing have traditionally used fault-tolerant computer systems for many years to ensure 100 percent availability. In online transaction processing, transactions entered online are immediately processed by the computer. Multitudinous changes to databases, reporting, and requests for information occur each Instant (Laudon and others, 2006).

Business continuity and disaster recovery planning supports this requirement by establishing thorough 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, or the performance of information technology functions using manual methods (Lennon, 2002).

Information technology leaders use business continuity and disaster recovery planning to create mechanisms for resuming partially or completely interrupted critical technology functions within a predetermined time after a disaster or disruption (Williamson, 2007).

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. Companies need 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 companies 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 companies survive long-term after a major incident (Snedaker, 2007).

Business continuity and disaster recovery plan is developed to prevent interruptions to normal business. If these events cannot be prevented, the goals of the plan are to minimize the outage and reduce the potential damage that such disruptions might cost the organization. Therefore, the business continuity and disaster recovery plan should also be designed to help minimize the cost associated with the disruptive events and mitigate the risks associated with these disruptive events. Disasters can be natural events; storms, floods, and so on; man-made events; computer viruses, malicious code, and so on; technical events; equipment failure, programming errors, and so on (Gregg, 2007).

Business continuity planning focuses on how the company can restore business operations after a disaster strikes. The business continuity plan identifies critical business processes and determines action plans for handling mission-critical functions if systems go down (Laudon and others, 2006).

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 (Laudon and others, 2006).

2.2 The Evolution of Business Continuity

Business continuity management is the outcome of a process that started in the early 1970s as computer disaster recovery planning and then moved through an era where the emphasis was on business continuity planning rather than on management (Gallagher, 2003).

In the 1970s the disaster recovery activity was driven by the computer manager. In realizing that the concentration of systems and data in itself created new risks, computer operations management introduced formal procedures governing issues such as back-up and recovery, access restrictions, physical security, resilience measures such as alternative power supply, and change control(Gallagher, 2003).

The interest in business continuity has gained significant momentum in the last several years, especially with the Year 2000 problem non-event. There are several reasons for this heightened interest, but probably the most significant reason is the increasing levels of devastation associated with recent disasters. In recent years we have witnessed a series of headline-grabbing, thought provoking disasters: hurricanes, power outages, floods, tornadoes, earthquakes, and ice and snow storms (Laudon and others, 2006).

In those days, if a major incident or disaster happened, the downtime that could be tolerated was measured in days rather than hours. Unsurprisingly, the cost of back-up computers sitting idle in an alternative location waiting for a disaster to happen was prohibitive.

However, organizations such as banks were in a more vulnerable position and invested considerable resources in installing and testing computers at alternative sites. Back-up tapes or disks were increasingly stored at protected locations well away from the computer centre (Gallagher, 2003).

The 1980s saw the growth of commercial recovery sites offering services, often on a shared basis. This was the start of the sophisticated recovery centers that operate today. However, the emphasis was still only on information technology. The disaster recovery plans documented the actions required to safeguard and restore computer operations. These covered computer processing, computer applications, telecommunications services and data after a disruptive event. The objectives were to prevent or at least minimize the impact that such an event would have on the business. They were more concerned with, for example, restoring a company's financial systems to an operational state than with worrying about whether there

would be accommodation available to allow the staff of the finance department actually to use the systems (Gallagher, 2003).

The 1990s witnessed significant change in the information technology environment and in the move from disaster recovery to business continuity. Throughout this decade, and into the 2000s, there were significant changes in the information technology approach to business continuity and disaster recovery planning and in what constituted acceptable downtime. The emphasis moved from being mainly on information technology to an approach that considered all aspects of an organization's business and relationships. Now business continuity has become business continuity with the emphasis on management, not just planning. This encompasses the emphasis on risk management and the measures to be taken to reduce risk. Business continuity and disaster recovery planning is no longer regarded as a project; it is now a program, emphasizing that it is a continuous process rather than a task with a defined end-date. After September 11 business continuity and disaster recovery planning has assumed a new importance. Board members now realize that the very survival of the enterprise may depend on it. The increased recognition of business continuity and disaster recovery planning means that a greater budget allocation may be available to it (Gallagher, 2003).

2.3 Impact Of year 2000

The hype, concerns, remedial action and contingency plans that surrounded the year 2000 problem had significant implications for business continuity and disaster recovery planning. In the first place, it was the fear and uncertainty concerning the implications of the year 2000 changeover that caused many organizations to think of business continuity and disaster recovery planning for the first time. In addition (Gallagher, 2003):

- It increased awareness of business interruption issues.
- It resulted in a better understanding of critical processes and vulnerabilities.
- It improved co-operation and collaboration between public and private sectors on emergency management issues.

The work that was done to ensure that systems addressed the date change correctly led to significantly better control over systems. Systems documentation was improved, and some organizations established a proper inventory of their systems and data for the first time. Most organizations had never previously realized the degree to which equipment and processes were dependent on a computer chip to function. The uncertainty surrounding the implications for embedded systems also resulted in significantly better records and understanding in this area. It

is considered to a large extent, before September 11, it was Year 2000 problem that provided the greatest boost to business continuity and disaster recovery planning. Many of those responsible for the Year 2000 problem project were then given the task of building on the work done and of broadening it out into full-scale corporate business continuity planning and management (Gallagher, 2003).

2.4 Business Continuity And Disaster Recovery Definition

The disaster recovery and business continuity concepts are widely used in the literature and have even been used interchangeably (Jacobs and Weiner, 1997). And there are some of authors motioned that obviously "Ask 20 different people for their concept of contingency planning and you will probably get 20 different answers." (Andrews, 1990).

This confusion arises from the fact that there is no single, widely agreed-upon definition outlined by some governing body (McCracken, 2005). Although such terms may mean different things to various organizations and authors also, there are common items that are readily apparent in both concepts that need to be distinguished (Barbara, 2006).

Many authors gave definitions for business continuity. Snedaker (2007) has defined Business continuity planning as "a methodology used to create and validate a plan for maintaining continuous business operations before, during, and after disasters and disruptive events". *And* "business continuity has to do with managing the operational elements that allow a business to function normally in order to generate revenues. It is often a concept that is used in evaluating various technology strategies".

Laudon and Laudon(2006) defined it as "Business continuity planning focuses on how the company can restore business operations after a disaster strikes. The business continuity plan identifies critical business processes and determines action plans for handling mission-critical functions if systems go down.

BSI(2006) defined the business continuity as "holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities".

Disaster recovery Journal (2006) defined the Business Continuity as "The ability of an organization to ensure continuity of service and support for its customers and to maintain its

viability before, after and during an event".

Botha and Von Solms (2004) defined the business continuity as "business continuity involves developing a collection of procedures for the various business units that will ensure the continuance of critical business processes while the data center is recovering for disaster."

And there are many authors gave definitions for Disaster Recovery: Hood (2005) has defined it as "Disaster recovery is part of business continuity, and deals with the immediate impact of an event. Recovering from a server outage, security breach, or hurricane all fall into this category. It is equally important to understand that disaster recovery is a subset of business continuity".

Disaster recovery Journal (2006) has defined it as "Activities and programs designed to return the entity to an acceptable condition. The ability to respond to an interruption in services by implementing a disaster recovery plan to restore an organization's critical business functions".

Chow (2000) has defined it as "disaster recovery is a concern for computer security that provides alternatives for businesses facing contingency events that could be detrimental to the functions normally performed"

Botha and Von Solms(2004) has defined it as "disaster recovery focuses mainly on the recovery of the information technology department and all related functions"

Barbara (2006) has defined disaster recovery usually has several discreet steps in the planning stages. Disaster recovery involves stopping the effects of the disaster as quickly as possible and addressing the immediate result. This might include shutting down systems that have been breached, evaluating which systems are impacted by a flood or earthquake, and determining the best way to proceed".

Business Continuity & Disaster Recovery Comparison

Despite many similarities exist between disaster recovery and business continuity, differences between them are founded. TABLE 2.1 illustrates the main differences found in the literature.

Table 2.1: Disaster Recovery and Business Continuity Planning Comparison

Characteristic	**Disaster Recovery**	**Business Continuity**
Practice	Standard	Better
Vision	Old	New
Focus	It	Business
Staff	It	Multi-disciplinary
Structure	Existing	New
Aim	Protect core operations	Protect organization
Emphasis	Recovery	Prevention
Recovery approach	Single-focus	Holistic
Reaction	Reactive	Proactive

(Adopted from Barbara 2006 Table 2, Disaster Recovery and business continuity Approaches Compared, Barbara, 2006)

It is obvious from this section that there is no widely common definition of business continuity and disaster recovery planning, because of lack of common terminology and less of researches done in this field, which shaping major inhibitors of this field.

From these definitions, it can be said that the disaster recovery planning is a subset of business continuity planning, but the term business continuity and disaster recovery planning is more popular business continuity, and the use of term business continuity alone may confuse the targeted group of respondents, so the term business continuity and disaster recovery planning will be used for the purposes of this study.

And despite there is no common agreed definition of business continuity and disaster recovery planning, the researcher extracted one definition from the previous literature for the purpose of this thesis, which will be used as a guidance and reference in this thesis.

The definition is: The business continuity and disaster recovery planning is the process of creating a valid and comprehensive plan for keeping the business functions in operating mode before, during and after the disaster strikes, through identifying the potential threats to a business, and its effect on business operations, and to find the strategies to mitigate and face these threats.

2.5 The benefits of an effective business continuity and disaster recovery planning program

All stakeholders benefit from having a well-implemented and properly documented business continuity and disaster recovery planning program. Internally, confusion regarding recovery duties, corporate disruptions and reliance on key individuals decrease and the safety

of employees is consequently provisioned for. Externally, benefits include increased corporate credibility. As such, implementing an effective business continuity and disaster recovery planning program in any organization results in numerous benefits, as defined below (Barbara, 2006).

Many authors wrote about the benefits of business continuity and disaster recovery planning programs, where some of them were internal benefits and the others were external. These major benefits are explained below:

- Elimination of possible confusion and error(Jacobs and Weiner, 1997)
- Reducing disruptions to corporate operations (Iyer and Bandyopadhyay, 2000).
- Documented alternatives during a catastrophe (Iyer and Bandyopadhyay, 2000).
- Reducing reliance on key individuals (Iyer and Bandyopadhyay, 2000).
- Proper data protection (Brabara, 2006).
- Employee safety (Brabara, 2006).
- Having an orderly recovery (Karakasidis, 1997).
- Increased credibility and value-added to the organization (Jacobs and Weiner 1997).

The BSI added the following benefits of business continuity and disaster recovery planning to the organization (BSI, 2006):

- The organization is able to proactively identify risks to its operation, and have in place a capability to mitigate and manage those risks.
- The organization maintains an ability to manage uninsurable risks, such as risk to reputation.
- The organization has in place an effective response to major disruptions.
- The organization is able to demonstrate that the program is credible through a process of exercising and auditing.
- The organization may have a competitive advantage, conferred by the demonstrated ability to maintain customer service, profitability and employment of its staff.
- The organization is able to demonstrate that the program is iterative and is embedded as good business practice.

2.6 Major Inhibitors of Business Continuity /Disaster Recovery

Although business continuity and disaster recovery planning allow firms to effectively recover from a disaster, major inhibitors to such strategies exist and include such factors as

properly justifying costs regarding a business continuity and disaster recovery planning program, corporate barriers including a lack of management support and resources, and a lack of common terminology and relevant research. These and other major inhibitors are explained below (Barbara, 2006).

a) Cost & ROI: Increasing exponentially over time, one of the most cited inhibitors in the literature is the issue of financial cost (Hawkins, Yen et al., 2000; Nahum, 2003, Pisselo, 2002). Not only do direct, tangible costs of implementation (e.g.: software, hardware, telecommunications and salaries) hinder the decision to adopt a business continuity and disaster recovery planning initiative, but indirect, intangible costs.

b) Lack of Management Support.

c) Low Priority: To be deemed successful, any corporate executive member wishing to institute a business continuity and disaster recovery planning program must think of the latter as a high priority prior to implementation.

d) Lack of Common Terminology: Contingency planning notions abound with multiple definitions of similar concepts found in this field As such, confusion is often the result from this lack of common terminology since the origins of the discipline may explain the causes of this latter.

e) Lack of Research: A consequence from the lack of common terminology is the lack of research. Some authors infer that contingency planning proponents have not done enough to further the understanding and consensus of proposed terminologies and best practices in the field leading to better and more thorough research (Botha and Von Solms, 2004).

g) Lack of Resources: Ensuring that sufficient resources, knowledgeable and trained on the contents of the program, are available and willing to participate in disaster recovery may impede a smooth transition to recovery (Rohde and Haskett, 1990).

2.7 Business Continuity and Disaster Recovery plan components

2.7.1. Project Initiation

Before the Business Continuity and Disaster Recovery process can begin, management must be on board. Management is ultimately responsible and must be actively involved in the process (Gregg, 2006).

The initial phase of Business Continuity and Disaster Recovery planning must define and establish the objectives that are aligned with the goals of company (Chow, 2000)

A project is defined as a set of tasks having a defined start and end point and specific objectives, requirements, and goals. Clearly, Business Continuity and Disaster Recovery planning qualified as projects under this definition. The Business Continuity and Disaster Recovery planning process can, and should, be constructed as a project plan and each component Business Continuity and Disaster Recovery can then be implemented as a project (Snedaker, 2007).

2.7.1.1. Project management techniques

Project management techniques such as task management, resource allocation, scheduling and budgeting constitute the foundation of proper planning, development and implementation of any project (Karakasidis, 1997; Chow, 2000). Ensuring that all resources (monetary, time and human) are properly managed throughout a Business Continuity and Disaster Recovery project translates into positive returns (Barbara, 2006).

The purpose of project management techniques is to clearly identify events such as project tasks to be completed, person-in-charge for the completion of project, the time frame or schedule of tasks, start and completion activities, and the budgets for each task. Thus, the planning process would be properly controlled and completed within the schedule and the budget (Chow, 2000).

2.7.1.2. Elements of Project Success

As with any information technology project, there are numerous elements that tend to contribute to the likelihood of success. Those factors will be discussed and how they relate, specifically, to Business Continuity and Disaster Recovery planning efforts. We'll continue by looking at the elements that plan should include, how to organize the project and the participating team, and how to develop success criteria so that the progress and recognize success can be marked (Snedaker, 2007).

Numerous studies through the years show there are a set of factors that, when present, tend to make projects more successful (Brandon,2006; Snedaker,2007).

- Executive Support
- User Involvement
- Experienced Project Manager
- Clearly Defined Project Objectives

- Clearly Defined Project Requirements
- Clearly Defined Scope
- Shorter Schedule, Multiple Milestones
- Clearly Defined Project Management Process

2.7.1.3. Executive Support

It is imperative that a contingency program be initiated, supported, approved and authorized by upper management as of the initial stages of implementation (Chow, 2000). Top management is the sole corporate entity that can provide and secure large amounts of resources, capital and time (Chow, 2000; Botha and Von Solms, 2004) within such Business Continuity and Disaster Recovery life cycle activities as planning, analysis, testing, and maintenance (Cerullo and Cerullo, 2004).

Support from the top is essential to identify operations which are critical for the company's survival under adverse conditions, to assign tasks to individuals, and to provide important information concerning significant business functions. Management support is also needed for disaster recovery funding. Most managers operate within budgetary constraints and carefully consider both costs and benefits before allocating resources. Their involvement in the planning process will educate them about the importance of Business Continuity and Disaster Recovery planning and mitigate their concern over whether the benefits gained from the use of Business Continuity and Disaster Recovery planning merit the cost of implementation. This, in turn, will encourage investment in Business Continuity and Disaster Recovery planning. Thus, management commitment has become an essential ingredient for successful Business Continuity and Disaster Recovery planning (Iyar and Bandyopadhyay, 2000).

Executive support for any information technology project is typically the number one success factor. It makes sense that support from the top of the organization for an information technology project tips the odds of success in your favor since executives have the ability to provide funding, resources, staffing, and political cover. If they are convinced there is a clear business need, they will go to bat for you and help ensure you get what you need to succeed (Snedaker, 2007).

In a similar vein, a lack of top management understanding also impedes the effective implementation of a Business Continuity and Disaster Recovery program (Pitt and Goyal, 2004).

Top management commitment can ensure the ongoing provision of resources and

money for developing, maintaining, and testing the Business Continuity and Disaster Recovery plan (Chow, 2000).

Executives understand business and finance, they don't necessarily understand technology. Many are comfortable using technology and a vast majority understanding the need to utilize technology effectively within an organization; few understand the terminology and the underpinnings of technology (Snedaker, 2007).

The greatest barrier to launching a successful Business Continuity and Disaster Recovery is the cost associated with the development and maintenance of the business continuity and disaster recovery. The reason is that the associated cost of Business Continuity and Disaster Recovery is deemed too great and Business Continuity and Disaster Recovery has no immediate return on investment. Therefore, adequate financial support must be obtained so as to make Business Continuity and Disaster Recovery a success (Chow, 2000).

2.7.1.4. User Involvement

User involvement consistently shows up in one of the top three spots on the list of success factors for information technology projects. Many technology projects have failed because users were not involved and key decisions were made that were directly counter to user needs and wishes. Clearly, you can create any solution you want but you can't force users to use it. You can't force users to understand and accept convoluted processes for doing their once-simple tasks, to flex around awkward requirements of the technology. Although there can be compelling business drivers that force users to change their processes and methods these should be created with user input and collaboration, not in the dark recesses of the information technology Department (Bardon,2006).

There are essentially two sets of users. The first set includes those who will be involved in planning the Business Continuity and Disaster Recovery project itself. These people may or may not be the same ones who will implement these plans should disaster strike. Therefore, you would do well to have both sets of users involved in this project (Snedaker, 2007).

2.7.1.5. Experienced Project Manager

The project manager is the leader of a team performing a project; and experienced project managers bring a wealth of knowledge and skill to the table. They often have had some formal project management training or education and they may have achieved a standardized certification in one or more methodologies. Most importantly, though, they have been in the trenches managing projects, and have realistic understanding of what it takes to get the job

done (Bardon, 2006; Snedaker, 2007).

When we're looking at Business Continuity and Disaster Recovery specifically, an experienced project manager is likely to be more effective at working across organizational boundaries and in bringing together a diverse group of people and interests. Working effectively with people at all levels of the organization and in all areas of the company is critical to the success of a Business Continuity and Disaster Recovery plan. An experienced project manager is more likely to understand how to navigate through the company different departments during the development and implementation of cross-departmental projects (Snedaker, 2007).

In addition, an experienced project manager will utilize a defined set of steps, a methodology, to deliver consistent results. Most experienced project managers have developed a system of defining and managing projects that delivers positive results. Many have spent years honing their methods to generate an optimal outcome. Most adhere, in general terms, to standardized methodologies but each experienced and successful project manager undoubtedly will have customized those methodologies to suit their specific needs. This is a key to delivering a successful Business Continuity and Disaster Recovery project plan (Snedaker, 2007).

2.7.1.6. Clearly Defined Project Objectives

A Business Continuity and Disaster Recovery program should be driven by business needs to consequently create a competitive advantage in the form of more resilient systems (Elliott, Swartz et al., 1999). Management will be increasingly committed if they perceive that organizational goals are aligned with Business Continuity and Disaster Recovery planning objectives (Wong, Monaco et al., 1994).

Clearly defined project objectives might sound incredibly obvious, clearly defined objectives are quite important because Business Continuity and Disaster Recovery plan must be scaled to the organization's unique needs. Without defining the objectives, you and your team might spend a disproportionate amount of time planning and implementing a part of the plan that is less important, or you might short-change a very important area (Snedaker, 2007).

One way the task of defining objectives can contribute to Business Continuity and Disaster Recovery success is to develop a high-level list of functional areas of the company and invite key people from those areas to help define the objectives. This accomplishes two critical project objectives: it ensures that all functional areas are included and it brings together the

people most able to develop appropriate objectives (Snedaker, 2007).

2.7.1.7. Clearly Defined Project Requirements

Project requirements typically involve date/time and cost issues, and developing clear and complete requirements can also make the difference between success and failure, especially for an information technology-related project. The requirements are those capabilities, attributes, and qualities that must be part of the final project deliverable. Defining these early in the project development cycle is important because going back to add them in later is inefficient, costly, and fraught with both errors and additional project risk. Requirements are not the same as project objectives. The objectives should drive the requirements. Objectives are what you want to accomplish, requirements are how you will accomplish those objectives (Bardon, 2006; Snedaker, 2007).

Requirements may have to be refined or developed later in the project definition process as details about the project become clear. However, clear requirements, before project work begins are absolutely critical to project success. Unclear requirements cause confusion, duplication of effort, rework, and wasted work (Snedaker, 2007).

2.7.1.8. Clearly Defined Scope

A project's scope is the work to be done and the things to work on. This scope is enclosed within a multidimensional boundary line that separates those things that are part of the project from other things that are not part of the project (Bardon, 2006). Scope typically is defined through the project's objectives. Making sure payroll can be run during a disaster may be one objective, making sure your company can still take, fulfill, and invoice customer orders is another objective. If these are the only two objectives for your Business Continuity and Disaster Recovery plan, you can fairly easily determine the project's scope. Therefore, clearly defined objectives lead to a clearly defined project scope (Snedaker, 2007).

2.7.1.9. Shorter Schedule, Multiple Milestones

After all the tasks are sequenced, a schedule can be developed. The difference between a network diagram and a schedule is that a schedule is calendar based and takes into account the length of work weeks and holidays (Bardon, 2006).

Studies have repeatedly shown that shorter schedules with more milestones generate more successful results; Milestones are project markers that help you gauge progress. Milestones are checkpoints that can help you stay on budget, on schedule, and on scope as your project progresses. The more milestones the project has, the more likely it is to be successful, because

the planner are consistently comparing where company stated, and wanted to be with where it actually are(Snedaker, 2007).

2.7.1.10. Clearly Defined Project Management Process

A clearly defined project management process typically goes hand-in-hand with an experienced project manager. As mentioned, an experienced project manager is likely to have a set of methods, procedures, and associated documents that he or she has used successfully in the past (Snedaker, 2007).

2.7.1.11. Project Plan Components

After that reviewing the success factors, let's look at standard project management plan components, the basic steps in a project are (Snedaker, 2007):

- Project Definition
- Forming the Project Team
- Project Organization
- Project Planning
- Project Implementation
- Project Tracking
- Project Close Out

Project planning and project management are both linear and iterative processes. This means that there is a logical flow that defines the order in which steps are taken; at the same time, many steps are revisited over time to add additional detail that helps more clearly define the project(Snedaker, 2007).

2.7.2. Risk Assessment

Before an organization commits resources to controls, it must know which assets require protection and the extent to which these assets are vulnerable. A risk assessment helps answer these questions and also helps the firm determine the most cost-effective set of controls for protecting assets (Laudon and Laudon, 2006).

Risk assessment typically focuses on potential business exposure to (Paton, 1999), and the ultimate objective of the risk assessment phase is to provide management with the necessary information to further evaluate - or analyze - each identified threat (Pitt and Goyal, 2004).

Risk assessment must be conducted within the first phases of the implementation cycle to systematically assess the potential impacts of all unexpected events to the organization (Smith, 1995).

A risk assessment determines the level of risk to the firm if a specific activity or process is not properly controlled. Business managers working with information systems specialists can determine the value of information assets, points of vulnerability, the likely frequency of a problem, and the potential for damage (Laudon and Laudon, 2006).

While assessing risks, it is important to consider all critical elements affecting an organization. Such factors as determining critical information systems , establishing recovery priorities and identifying target recovery times for each application need to be taken into account (Hawkins, Yen et al., 2000; Savage, 2002; Castillo, 2004).

The risk assessment considers all possible threats to the information system, such as natural disaster, hardware and software failure, and human error (Chow, 2000)

A control weakness at one point may be offset by a strong control at another. It may not be cost-effective to build tight controls at every point in the processing cycle if the areas of greatest risk are secure or if compensating controls exist elsewhere. The combination of all of the controls developed for a particular application determines the application's overall level of control (Laudon and Laudon, 2006).

2.7.2.1. Risk Management Process

The process of managing risk includes assessing potential and also analyzing the trade-offs, or opportunity cost. The principal goal of an organizations risk management process should be to protect the organization and its ability to perform their mission, not just its information technology assets. Therefore, the risk management process should not be treated

primarily as a technical function carried out by the information technology experts who operate and manage the information technology system, but as an essential management function of the organization (Stoneburner and others, 2001).

Imagine a company that says we need to make sure our systems never go down. The potential for systems to go down occasionally is very high; most systems go down for one reason or another from time to time. The cost of those system outages varies, usually in direct correlation to the time the system is down. If the system is down for 10 minutes while it's rebooted due to an emergency patch installation, the cost may be negligible. If the system goes down for days because the database is corrupted by a hacker and restoring back to the previously validated database data experiences a few problems, the cost is much higher (Snedaker, 2007).

2.7.2.2. Risk Management objectives

The objective of performing risk management is to enable the organization to accomplish its mission(s) by (Stoneburner and others, 2001):

- Better securing the information technology systems that store, process, or transmit organizational information.
- Enabling management to make well-informed risk management decisions to justify the expenditures that are part of an information technology budget.
- Assisting management in authorizing (or accrediting) the information technology systems on the basis of the supporting documentation resulting from the performance of risk management.

2.7.2.3. Threat Assessment

Risk assessment is the first process in the risk management methodology. Organizations use risk assessment to determine the extent of the potential threat and the risk associated with an information technology system, the output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process (Stoneburner and others, 2001).

Risk management is about trying to manage uncertainty. We can't ever completely remove all risk all the time, but we can find ways to reduce or eliminate many risks to some degree. The process of risk management is the process of determining which risks should be addressed and how they should be addressed (Snedaker, 2007).

By identifying specific threats to business operations and measuring each one's

probability of occurrence, specific methodologies can be applied to justify the budget to find avoidance controls (Barbara, 2006).

Both business risk and information technology-specific risk must be addressed using the same methodology, only the details will differ. We can use the following equation to define risk as well:

Risk = Threat + (Likelihood + Vulnerability) + Impact

So in other words we can say that, Risk is a function of the likelihood of a given threat-sources exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization (Stoneburner and others, 2001).

Thus, risk could be viewed as the combination of the threat itself, the likelihood of that threat occurring, the vulnerability of the organization or system to that threat, and the relative or absolute impact of that threat on the organization or system. Likelihood and vulnerability are shown in parentheses simply to indicate that some people prefer to assess these in one pass or as one value (Snedaker, 2007).

2.7.2.4. Vulnerability Assessment

Vulnerability is a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the systems security policy (Stoneburner and others, 2001).

The vulnerability assessment analyzes how vulnerable, susceptible, and exposed a business or system is to a particular threat. It should include an assessment of how vulnerable a particular system is to a threat as well as the likelihood of that threat occurring. The likelihood portion of the assessment can be part of the vulnerability assessment, though the planner could also break it out as a separate process if desired. As long as risk assessment includes vulnerability and likelihood assessments, you should be in good shape (Snedaker, 2007).

The goal of this step is to develop a list of system vulnerabilities (flaws or weaknesses) that could be exploited by the potential threat-sources (Stoneburner and others, 2001).

The vulnerability and the likelihood of the event are closely related and the results are used as inputs to the impact assessment. Certainly, a server that is outside the firewall is far more vulnerable to external attacks than a server inside the firewall. This is an example of relative vulnerability since both servers are vulnerable but one more so than the other. How likely either server is will be attacked? Probably 100% for the server outside the firewall and

perhaps 90% for the server inside the firewall in today's attack-laden environment. As seen, creating relative assessments for vulnerability and likelihood result in different risk profiles for the two servers (Snedaker, 2007).

2.7.2.5. Information Technology Specific Risk Management

Risk management across the business enterprise is a wide and varied topic, information technology-specific risk management is a subset of overall business risk management. That said, there are some very unique risks in information technology that exist nowhere else in the enterprise (Snedaker, 2007).

Identifying risk for an information technology system requires a keen understanding of the systems processing environment. The person or persons who conduct the risk assessment must therefore first collect system-related information, which is usually classified as follows ((Stoneburner and others, 2001):

- Hardware
- Software
- System interfaces (e.g., internal and external connectivity)
- Data and information
- Persons who support and use the information technology system
- System mission (e.g., the processes performed by the information technology system)
- System and data criticality (e.g., the system.s value or importance to an organization)
- System and data sensitivity.

The operating environment data can include (Snedaker, 2007):

- The functional requirements of the information technology system
- The technical requirements of the system
- Users of the system
- www Security policies (company policies, industry, regulatory, governmental requirements)
- Security architecture (to assess vulnerability to cyber threats)
- Level of protection needed for confidentiality, integrity, and availability
- Current network topology, network diagrams
- System interfaces, information flow diagrams
- Data storage protection

- Technical controls (added security products, identification requirements, access requirements, audits, encryption methods, etc.)
- Physical controls (access control, monitoring, etc.)
- Organizational controls (policies and procedures defining acceptable methods and behaviors)
- Operational controls (backup policies and procedures, personnel security, system maintenance, off-site storage or computing capabilities, etc.)
- Environmental controls (power, temperature, humidity)

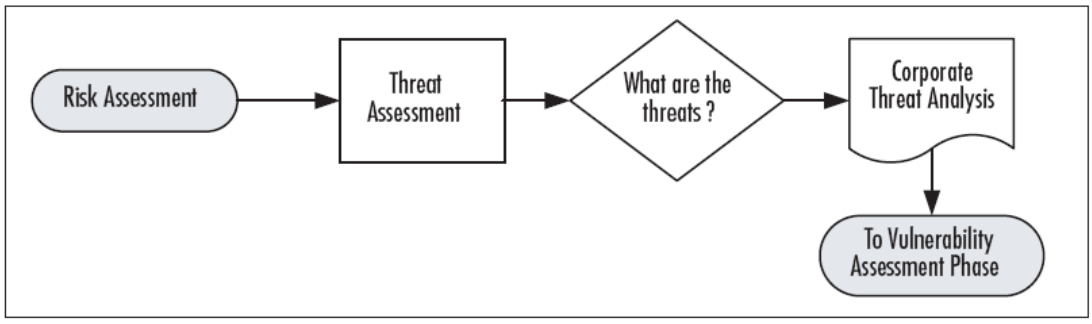
These items are included to give the planner additional insights into the areas need to be investigated throughout risk assessment phase. Some items may not be relevant, and it can be deleted from the list. The planner may have other items not listed that you want to include (Snedaker, 2007).

2.7.2.6. Risk Assessment Components

The risk assessment begins with the assessment of all potential threats and an analysis of those threats. The output from this phase is the input to the vulnerability assessment phase.

In Business Continuity and Disaster Recovery planning, understanding the threats and threat sources can help in uncovering potential risks to the company or information technology systems about which were previously unaware (Snedaker, 2007).

Figure 2.1: Risk Assessment Sub-process



(Adopted from Snedaker 2007 Fig3.3, Risk Assessment Sub-process, Snedaker, 2007)

2.7.2.7. Information Gathering Methods

Information is gathered principally through interviews and/or surveys with the resource(s) most implicated with the concerned application(s) or system(s). Results include detailed cost/benefit breakdowns (Paton, 1999), desired recovery time objectives, classification

schemes of application/system criticality (Cerullo and Cerullo, 2004) and established frameworks of risks (Iyer and Bandyopadhyay, 2000).

2.7.2.8. Threat Checklist

The list, shown in **Table 2.2**, is provided for your convenience. It is a reiteration of all the threats listed in the previous sections. You may want to use this list as a starting point in your threat assessment. You can add any threats not included in the list and remove those you're confident will not impact your business.

Table 2.1 Threat Checklist

Natural/Environmental Threats
Fire (can be human-caused)
Flood
Severe winter storm
Electrical storm
Drought
Earthquake
Tornado
Human-Caused Threats
Fire, Arson
Theft, Sabotage, Vandalism
Labor disputes
Workplace violence
Terrorism
Chemical and biological hazards
War, Civil unrest
Infrastructure Threats
Building-specific failures
Non-information technology equipment, System failures
Heating/Cooling, Power failures
Public transportation disruption
Oil, petroleum supply disruption
Regulatory, legal changes

(Adopted from Snedaker 2007 Table 3.2, information technology-Specific Threats, Snedaker, 2007)

Table 2.2 Information Technology Specific Threats

Threat To	Specific Threats
Hardware	Equipment failure (intentional, unintentional damage)
	Power outage
	Equipment reconfiguration
	(authorized, no authorized)
	Equipment sabotage
	Equipment theft
Software	Bugs, glitches
	Data corruption
	Data security breach (deleted, stolen, modified)
	System configuration changes (errors or sabotage)
Infrastructure	Internet connection(s)—failure, tampering, destruction
	Wireless networks—failure, tampering, destruction
	Network backbone—failure, tampering, destruction
	Cabling—failure, tampering, destruction
	Routers, infrastructure hardware—failure, tampering, Destruction.

(Adopted from Snedaker 2007 Table 3.3, information technology-Specific Threats, Snedaker, 2007)

2.7.2.9. Threat Assessment Methodology

Before we head into the vulnerability assessment phase, we're going to discuss threat assessment methodologies that might be useful to you in evaluating various threats. In essence, there are two ways you can approach this. The first is to use a *quantitative* approach, in which you attempt to use hard numbers to represent threats, vulnerabilities, and impacts. In some companies, this may be the norm or it may be required for some reason. The second method is a qualitative approach, where you attempt to define the relative threats, vulnerabilities, and impacts. You use qualitative or value-based language such as "high,""medium," and "low"(Snedaker, 2007).

2.7.3. Business Impact Analysis

Chance and uncertainty are part of the world we live in. We cannot predict what tomorrow will bring or whether a disaster will occur but this doesn't mean that we cannot plan for it (Gregg, 2006).

Impact analysis evaluates all feasible risks to determine the vulnerability of each threat to the organization. (Grillo, 2003)

At a basic level, business impact analysis is a mean of systematically assessing the potential impacts resulting from various events or incidents that might cause existing facilities or systems to be unavailable (Savage, 2002).

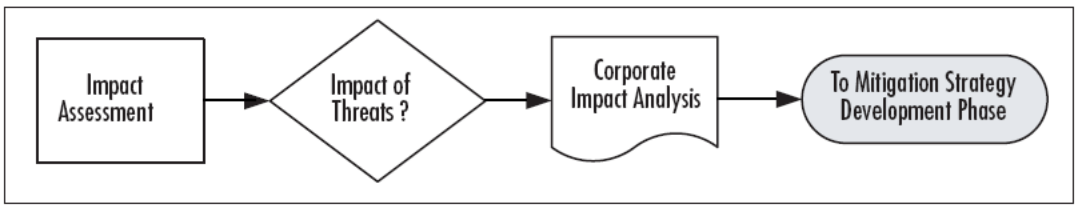
Risk assessment looks at the various threats the company faces, business impact analysis looks at the critical business functions and the impact of not having those functions available to the firm. These two assessments look at the company from two different angles. The risk assessment starts from the threat side, and the business impact analysis starts from the business process side (Snedaker, 2007).

During the business impact analysis phase critical business processes are identified and then analyzed. Once the analysis is complete, the impact that various disasters may have on business should become clear (Botha and Von Solms, 2004).

The business impact analysis should present a clear picture of what is needed to continue operations if a disaster occur. The individuals responsible for the business impact analysis must look at the organization from many different angles and use information from a variety of inputs. For the business impact analysis to be successful, the business impact analysis team must know what key business processes are (Gregg, 2006).

Business impact analysis helps the organization to understand the degree of potential loss (and other undesirable effects) which could occur (Savage,2002).

Figure 2.2 Impact Assessment Process



(Adopted from Snedaker 2007 Fig. 4.2, Impact Assessment Process, Snedaker, 2007)

The fundamental task in business impact analysis is understanding which processes in the business is vital to ongoing operations and to understand the impact the disruption of these processes would have on the business.

A simple way to examine such impact is to identify the key business processes and then to examine the effects of possible emergency/ disaster scenarios on each of them (Savage, 2002).

From an information technology perspective, as the National Institute of Standards and Technology views it:" The business impact analysis purpose is to correlate specific system components with the critical services that they provide, and based on that information, to characterize the consequences of a disruption to the system components."(Marianne, 2006).

As an information technology professional, the importance of various information technology systems should be certainly understood, but it may not be fully awarded of the critical business functions performed in the company (Snedaker, 2007).

2.7.3.1. Business impact analysis purposes

According to the Business Continuity Institute, a recognized leader in business continuity management and certification, there are four primary purposes of the business impact analysis (BCI, 2006):

- Obtain an understanding of the organization's most critical objectives, the priority of each, and the timeframe for resumption of these following an unscheduled interruption.
- Inform a management decision on Maximum Tolerable Outage for each function.
- Provide the resource information from which an appropriate recovery strategy can be determined/ recommended.
- Outline dependencies that exist both internally and externally to achieve critical objectives.

2.7.3.2. Understanding Impact Criticality

While the planner is thinking about the company and its critical functions, he should keep a rating scale in mind. Later, after he has compiled his list, he can assign a "criticality rating" to each business function. It's important to have an idea of his rating system in mind before reviewing his business functions so he can spend the appropriate amount of time and energy on mission-critical functions and less time on minor functions (Snedaker, 2007).

2.7.3.3. Criticality Categories

The planner can develop any category system that works for him but as with all rating systems, be sure the categories are clearly defined and that there is a shared understanding of the proper use and scope of each. Here is one commonly used rating system for assessing criticality (Snedaker, 2007):

- Category 1: Critical Functions–Mission-Critical
- Category 2: Essential Functions–Vital
- Category 3: Necessary Functions–Important
- Category 4: Desirable Functions–Minor

Obviously, the business continuity plan will focus the most time and resources on analyzing the critical functions first, essential functions second. It's possible to delay dealing with necessary and desirable functions until later stages of the business recovery (Snedaker, 2007).

2.7.3.4. Recovery Time Requirements

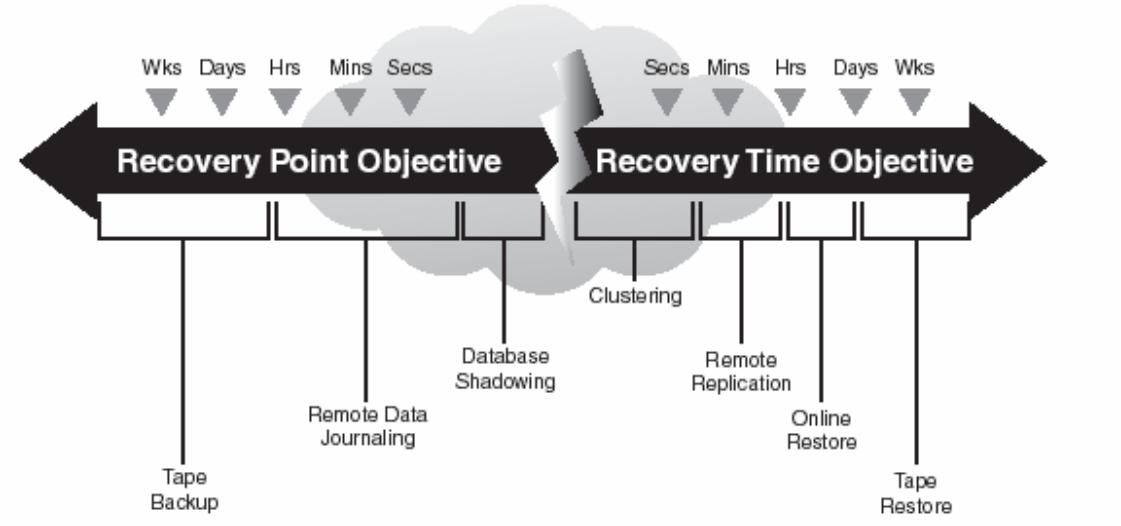
The impact analysis evaluates the consequences of an information system disaster in each functional area of the business and assesses the maximum allowable information system downtime (Chow, 2000).

Related to impact criticality are recovery time requirements. Let's define a few terms here that will make it easier throughout the rest of the analysis to talk in terms of recovery times.

Maximum Tolerable Downtime, the maximum time a business can tolerate the absence or unavailability of a particular business function. Different business functions will have different Maximum Tolerable Downtimes. If a business function is categorized as mission-critical, it will likely have the shortest Maximum Tolerable Downtime. There is a correlation between the criticality of a business function and its maximum downtime. The higher the criticality, the shorter the maximum tolerable downtime is likely to be. Downtime consists of two elements, the systems recovery time and the work recovery time. Therefore, Maximum Tolerable Downtime = Recovery Time Objective + work recovery time (Snedaker, 2007).

Recovery Time Objective: The time available to recover disrupted systems and resources (systems recovery time). It is typically one segment of the Maximum Tolerable Downtime. For example, if a critical business process has a three-day Maximum Tolerable Downtime, the Recovery Time Objective might be one day (Day 1).This is the time you will have to get systems back up and running. The remaining two days will be used for work recovery (Snedaker, 2007).

Figure 2.3: **Recovery Point Objective and Recovery Time Objective**



(Adopted from Gregg, 2006 Fig. 9.3, RPO and RTO, Gregg, 2006)

Work Recovery Time: The second segment that comprises the maximum tolerable downtime. If the Maximum Tolerable Downtime is three days, Day 1 might be your Recovery Time Objective and Days 2 to 3 might be the Work Recovery Time. It takes time to get critical business functions back up and running once the systems (hardware, software, and configuration) are restored (Snedaker, 2007).

Recovery Point Objective: the amount or extent of data loss that can be tolerated by the critical business systems. For example, some companies perform real-time data backup, some perform hourly or daily backups, some perform weekly backups. If you perform weekly backups, someone made a decision that the company could tolerate the loss of a week's worth of data. If backups are performed on Saturday evenings and a system fails on Saturday afternoon, the company has lost the entire week's worth of data. This is the recovery point objective. In this case, the Recovery Point Objective is one week. If this is not acceptable, the current backup processes must be reviewed and revised. The Recovery Point Objective is based both on current operating procedures and the estimates of what might happen in the event of a business disruption (Snedaker, 2007).

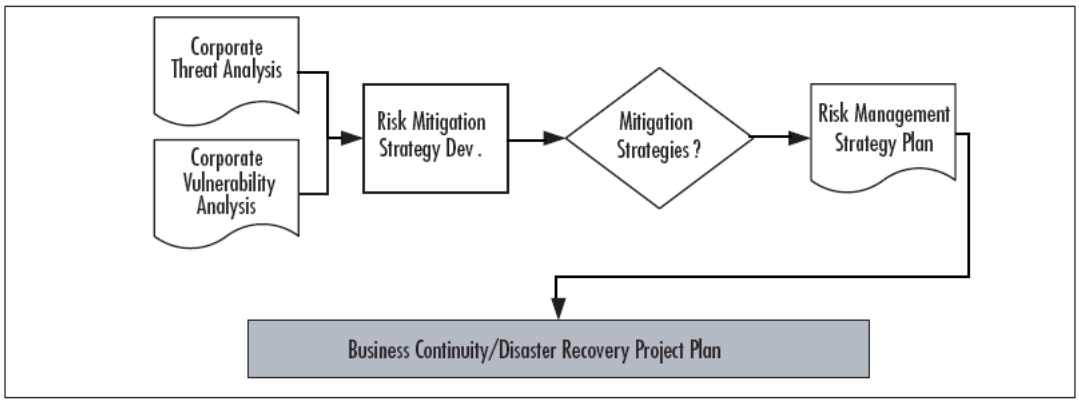
When the maximum allowable information system downtime is determined, management will be much more inclined to defend the resources required to maintain the recovery facilities, and to plan as necessary to enable recovery within the tolerance period(Chow,2000).

2.7.4. Mitigation Strategy Development

Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process (Stoneburner and others, 2001).

Data gathering phase has concluded and now it's time to put all this data to work. The mitigation strategy development phase of the business continuity and disaster recovery project plan is where development of strategies to accept, avoids, reduce, or transfer risks related to potential business disruptions. Developing the risk mitigation strategies is the last phase of risk management activities. This last segment includes the inputs of the risk assessment and business impact analysis data. This information, along with risk mitigation data, is used to develop strategies for managing risks in a manner that is appropriate for the company. Once the planner has the risk management section completed, he can begin to draft his business continuity and disaster recovery plan (Snedaker, 2007).

Figure 2.4 Risk Mitigation Strategy Development Phase



(Adopted from Snedaker 2007 Fig. 5.2, Risk Mitigation Strategy Development Phase, Snedaker, 2007)

2.7.4.1. Types of Risk Mitigation Strategies

There are four standard choices: acceptance, avoidance, limitation, and transference.

2.7.4.1.1. Risk Acceptance

To accept the potential risk and continue operating the information technology system or to implement controls to lower the risk to an acceptable level.

Risk acceptance is not really a mitigation strategy because accepting a risk does not reduce its effect. However, risk acceptance is part of risk management. There are various reasons why companies may choose risk acceptance in certain situations. The most common

reason is that the cost of other risk management options, such as avoidance or limitation, may outweigh the cost of the risk itself (Snedaker, 2007; Stoneburner and others, 2001).

2.7.4.1.2. Risk Avoidance

To avoid the risk by eliminating the risk cause and/or consequence, it is the opposite of risk acceptance because it's an all-or-nothing kind of stance in business continuity and disaster recovery plans, risk avoidance is the action that avoids any exposure to the risk whatsoever. Risk avoidance is usually the most expensive of all risk mitigation strategies, but it has the result of reducing the cost of downtime and recovery significantly. This option is not feasible for many types of risks or for many types of companies (Snedaker, 2007; Stoneburner and others, 2001).

2.7.4.1.3. Risk Limitation

To limit the risk by implementing controls that minimize the adverse impact of threats exercising vulnerability (e.g., use of supporting, preventive, detective controls), it is the most common risk management strategy employed by businesses. Companies choose to limit its exposure through taking some action. For example, performing daily backups of critical business data is a risk limitation strategy. It doesn't stop a disk drive from crashing, it doesn't ignore the potential for disk failure, it accepts that drives fail and when they do, having backups helps you recover in a timely manner. Risk limitations include installing firewalls to keep networks safe, creating backups to keep data safe, practicing fire drills to keep employees safe, and more(Snedaker, 2007 ; Stoneburner and others, 2001).

2.7.4.1.4. Risk Transference

To transfer the risk by using other options to compensate for the loss, such as purchasing insurance. Many companies outsource certain operations such as customer service, order fulfillment, or payroll services. They do this in many cases so they can focus on their core competencies, but they can also do this as part of risk management (Snedaker, 2007; Stoneburner and others, 2001).

The goals and mission of an organization should be considered in selecting any of these risk mitigation options. It may not be practical to address all identified risks, so priority should be given to the threat and vulnerability pairs that have the potential to cause significant mission impact or harm. Also, in safeguarding an organizations mission and its information technology systems, because of each organization unique environment and objectives, the option used to

mitigate the risk and the methods used to implement controls may vary (Stoneburner and others, 2001).

2.7.4.1.5. information technology Risk Mitigation

Although the technology used in a company will change over time and may not be the same as that discussed here, Risks to data include not only the natural disasters, but data disruptions and outages due to data center outages (fire, power, etc.); hardware or software failures; network security breaches; data security breaches that can include lost, stolen, modified, or copied critical data; and disruption due to critical data not being available to legitimate users (Denial of Service attacks, etc.).Risk and impact assessments should have covered these areas and this is a good time to check to ensure all data risks are addressed (Snedaker, 2007).

2.7.4.2. Critical Data and Records

Ensuring that all critical information, activities, systems, and material is properly backed up and stored off-site is of prime importance to the effectiveness of the Business Continuity and Disaster Recovery program and the continuous operation of the business when disaster strikes (Rohde and Haskett, 1990).

In today's information technology-dependent world, performing routine information and equipment backups via detailed procedures and storing them off-site through various networking means is becoming an increasing reality. Relying upon live, up-to-the-minute information is critical for corporations to sustain a competitive advantage (Jacobs and Weiner, 1997).

2.7.4.3. Critical Systems and Infrastructure

Once the planner understands his data management and data protection needs within the scope of the Business Continuity and Disaster Recovery planning process, he can begin to evaluate hardware and software solutions, vendors, and costs. There is no magic solution that will cover all company needs and if he has been working in information technology for any length of time, he already know that painfully well(Snedaker, 2007).

2.7.4.4. Information Technology Recovery Systems

Selecting an appropriate backup site involves prior analysis of corporate risks and business processes, determination of the criticality and degree of dependency on information technology and knowledge of the length of maximum allowable downtime of critical systems

(Chow, 2000). This ensures that all mission-critical information and equipment are appropriately safeguarded from any possible loss or damage (Iyer and Bandyopadhyay, 2000; Savage, 2002). This full recovery strategy includes preliminary measures, descriptive recovery procedures, selection of an appropriate backup site and detail of backup and off-site storage requirements of vital information and equipment (Savage, 2002).

2.7.4.4.1. Alternate Sites

Off-site storage, such as backup hardware, software, data files, and source documents, is a vital part of effective Disaster recovery planning because it allows a company to recover their relevant information if a disaster strikes (Chow, 2000).

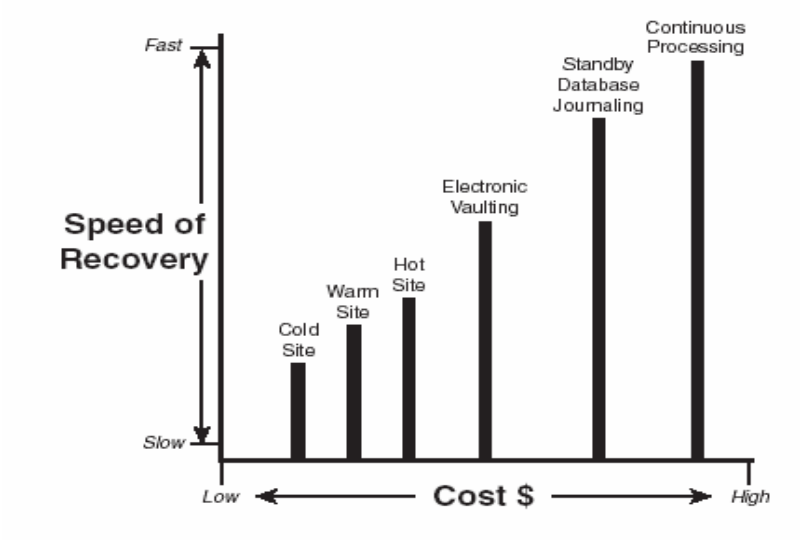
2.7.4.4.2. Fully Mirrored Site

A fully mirrored duplicate site allows for instantaneous and perhaps, even automatic switching between the live site and the back-up site if the live site fails for any reason. This is normally the most expensive option but may be appropriate (and not overly expensive) for an e-commerce Website (Savage, 2002).

2.7.4.4.3. Hot Site

This is an alternative outsourcing arrangement with a commercial vendor who maintains a compatible site to enable information technology operations to be transferred to that site and commissioned within an agreed time period, usually of the order of one working day (Savage, 2002).

Fig 2.5 Recovery options and cost



(Adopted from Gregg, 2006 Fig. 9.4, RPO and RTO, Gregg, 2006)

2.7.4.4.4. Warm Site

This location offers significantly less opportunity for success. Warm sites are typically shell buildings with basic utility services and require extra time to make ready. Computer equipment may not be on-site yet, or may require configuration before it is ready to use. After several hours of system configuration, additional delays will occur as data files are loaded. Communication lines will need to be activated and traffic rerouted before the voice and data can go online. This type of site will be operational in a matter of days or weeks. The location may be a branch office of the same organization (Canon and others, 2006).

2.7.4.4.5. Switchable (Mobile) hot site.

This is an outsourcing arrangement with a commercial vendor who will guarantee to maintain an identical site with appropriate communications so that information technology operations can be switched to that site within an agreed, short time period, usually less than one to two hours (Savage, 2002). Many professionals consider the mobile site to be a derivative of the cold site, with no guarantee of timely service. If a mobile site can be reliably obtained, a practical application may be to use the site as an interim facility for the months after leaving a hot site, but before reoccupying a permanent site (Canon and others, 2006).

2.7.4.4.6. Cold Site

A cold site is started up “cold” in the aftermath of a disruption. These kinds of sites are the least expensive in advance of an emergency but take the longest to bring online after a disruption, this strategy involves the setting up of an emergency site once the crisis has occurred and involves an "on call" arrangement with a commercial vendor to provide the minimum configuration urgently - this usually allows systems to be established and working within two to three working days (Savage, 2002).

2.7.4.4.7. Disk Systems

Disk systems solutions continue to evolve in terms of capabilities. They also tend to become less expensive over time as well. We’ll take a quick look at some of the solutions available to you today (Snedaker, 2007).

2.7.4.4.7.1. RAID

Redundant arrays of inexpensive disks come in several forms. The ability to hot-swap disks from a RAID array can be an important attribute of the disk recovery strategy (Snedaker, 2007). This is achieved by breaking up the data and writing it to multiple disks.

To applications and other devices, RAID appears as a single drive. Most RAID systems have hot-swappable disks, which mean that the drives can be removed or added while the computer systems are running (Savage, 2002).

2.7.4.4.7.2. Data backup strategy

Every recovery strategy requires data to be kept on backup tapes. The typical data backup strategy implements one of the following methods (Canon and others, 2006):

Full backup creates an entire copy of each file on the system. This is the most effective backup method and requires a significant amount of time.

Incremental method Copies only the files that have changed since the last backup. The incremental method is commonly used for backups on weekdays. This method requires less time than a full backup. Unfortunately, the file restoration process takes longer because it is necessary to restore the full backup and each version of incremental backup. An incremental backup resets the archive bit (backup flag) to indicate that a file needs to be backed up.

Differential method Copies every file that has changed between full backup runs. Differential is the preferred method for business continuity. This method ensures that multiple copies of daily files should exist on multiple tapes. A differential backup is very fast on the first day after a full backup, and then takes longer each day as more files are copied. A differential backup does not change the archive bit (backup flag). When selecting the data backup strategy, it is important to consider the time necessary for data restoration. Care should be given to ensure the RTO and RPO are met (Canon and others, 2006).

2.7.4.4.8. Remote Journaling

Remote journaling refers to the parallel processing of transactions to an alternate site, as opposed to a batch dump process like electronic vaulting. A communications line is used to transmit live data as it occurs. This feature enables the alternate site to be fully operational at all times and introduces a very high level of fault tolerance (Krutz, 2007).

2.7.4.4.9. Replication

Disk replication involves copying data on to a primary and secondary server. Shadowing and Clustering are two methods of accomplishing replication. Shadowing happens asynchronously, changes are collected and applied to the secondary server periodically. Shadowing can be part of a risk mitigation strategy, but keep in mind that any corruption or error on the primary server will be replicated to the secondary server. Clustering is a higher-end solution than shadowing and it provides high availability. Server clustering works in a manner

similar to RAID for disk drives. With clustering, several servers are tied together and periodically synchronize with one another. If a server goes down, the workload shifts to the remaining servers. This process is transparent to users who connect to the application and have no idea which server is providing data. And clusters provide load balancing for users and this same functionality provides a level of risk mitigation as well (Snedaker, 2007).

2.7.4.4.10. Electronic Vaulting

Electronic vaulting refers to the transfer of backup data to an off-site location. This is primarily a batch process of dumping the data through communications lines to a server at an alternate location (Krutz, 2007).

Data is sent directly from the subscriber site to the hot site. This costly service requires that a direct-access storage device be dedicated to the subscriber, preventing the service from being shared with other subscribers (Noakes, 2003).

2.7.4.4.11. Standby Operating Systems

It is the process of having the operating system loaded and ready in a disk that can be attached to the machine at the alternate site. This method, when used with other techniques, can save the time and effort required getting the operating system ready in the backup server, after a disaster (Ramesh,2002).

2.7.4.4.12. Desktop Solutions

Organization should already have some process in place for backing up user data. In the Microsoft Windows operating system, most users save data to the My Documents folder or to a designated network location. For enterprise applications, user data may be stored more centrally. Regardless of the configuration, it's important that critical user data be backed up periodically. Ideally, this process should be automated so it does not rely on user compliance with established backup processes. Backups of user data should also be stored securely offsite (Snedaker, 2007).

Considerations for desktop and portable systems should emphasize data availability, confidentiality, and integrity. To address these requirements, the systems manager should consider each of the following practices (Swanson, 2002):

- Store Backups Offsite.
- Encourage Individuals to Back Up Data.
- Provide Guidance on Saving Data on Personal Computers.
- Standardize Hardware, Software, and Peripherals.

- Document System Configurations and Vendor Information.
- Coordinate With Security Policies and System Security Controls.
- Use Results From the business impact analysis.

2.7.4.4.13. Software and Licensing

These are procured initially at a cost and so must be backed up and stored at an offsite storage location (Ramesh,2002).

2.7.4.4.14. Web Sites

There are two primary risks related to corporate Web sites. The first is the security risk due to the nature of external (public) Web sites. Risk mitigation strategies for Web sites include implementing strong security measures along with auditing and monitoring activity on the server. In addition, many corporate Web sites are used to conduct e-commerce transactions and the disruption of these transactions can have a significant impact on revenue streams and on customer perception of the company. Some companies use load balancing strategies to ensure Web sites have high availability, and these same strategies also act as excellent risk mitigation strategies (Snedaker, 2007).

Practices for Web site contingency planning include the following (Swanson, 2002):

- Document Web Site.
- Web Site Programming.
- Web Site Coding.
- Coordinate Contingency Solutions With Appropriate Security Policies and Security Controls.
- Coordinate Contingency Solutions with Incident Response Procedures.
- Use Results From the business impact analysis.

2.7.5. Business Continuity/Disaster Recovery Plan Development

Business Continuity Plan development refers to using the information collected in the business impact analysis to create the recovery strategy plan to support these critical business functions. Here the planner takes the information gathered from the business impact analysis and begins to map out a strategy for creating continuity plan (Krutz, 2007).

The risk analysis performed, led into vulnerability assessment. That data helped the planner to develop an assessment of the impact various risks would have on his business. Finally, he took all his data and identified mitigation strategies, actions he could take to avoid, reduce, transfer, or accept the various found risks. With that, he now have to develop a plan that takes his mitigation strategies and identifies both methods for implementing those strategies, and people, resources, and tasks needed to complete these activities. The plan basically needs to state 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. In some cases, there will be multiple mitigation strategies, in other cases, he may has elected to simply accept the risk (Snedaker, 2007).

2.7.5.1. Phases of the Business Continuity and Disaster Recovery

Hopefully company will never need to put it's Business Continuity and Disaster Recovery plan into action, despite all the hard work putted into it. If the company needs to use the plan, however, it will need to have clear and specific guidelines for how and when to implement it.

2.7.5.1.1. Activation Phase

The Notification/Activation Phase defines the initial actions taken once a system disruption or emergency has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, assess system damage, and implement the plan. At the completion of the Notification/Activation Phase, recovery staff will be prepared to perform contingency measures to restore system functions on a temporary basis (Swanson, 2002).

2.7.5.1.2. Recovery Phase

The recovery phase is the first phase of work in the immediate aftermath of the disruption or disaster. This phase usually assumes that the cause of the disruption has subsided, stopped, or been contained, but not always. This phase may include evacuating the facility, removing equipment that can be salvaged quickly, assessing the situation or damage, and

determining which recovery steps are needed to get operations up and going again (Snedaker,2007).

Recovery operations begin after the contingency plan has been activated, damage assessment has been completed (if possible), personnel have been notified, and appropriate teams have been mobilized. At the completion of the Recovery Phase, the information technology system will be operational and performing the functions designated in the plan. Depending on the recovery strategies defined in the plan, these functions could include temporary manual processing, recovery and operation on an alternate system, or relocation and recovery at an alternate site(Swanson, 2002).

2.7.5.1.3. Business Continuity Phase

The business continuity phase kicks in after the recovery phase and defines the steps needed to get back to "business as usual." The business continuity phase would address how actually to begin to resume operations from that temporary location, what work-arounds need to be implemented, what manual methods will be used in this interim period, and so forth. The final steps in the business continuity phase will address how business move from that temporary location to the repaired facility, how to reintegrate or synchronize data, and how to transition back to the normal operations (Snedaker, 2007).

2.7.5.1.4. Maintenance/Review Phase

The maintenance phase has to occur whether Business Continuity and Disaster Recovery plan ever activated or not. On a periodic basis, Business Continuity and Disaster Recovery plan need to be reviewed to ensure that it is still current and relevant. One common problem in Business Continuity and Disaster Recovery planning is that companies may expend time to develop a plan but they often do not want to (or will not) expend the time and resources necessary to keep the plan current. Old plans are dangerous because they provide a false sense of security and may lead to significant gaps in coverage. If a plan is not maintained, then all the time and money invested in creating the plan is wasted as well (Snedaker, 2007).

2.7.6. Business Continuity and Disaster Recovery Plan Testing, Auditing, and Maintenance.

2.7.6.1. Business Continuity and Disaster Recovery Plan Testing

A Business Continuity and Disaster Recovery planning becomes obsolete very quickly if it is not periodically tested. Therefore, a series of test programs needs to be developed and conducted to make sure the Business Continuity and Disaster Recovery planning is complete and accurate(Chow,2000).

If not thoroughly tested on a periodic and regular basis, a Business Continuity and Disaster Recovery plan quickly becomes obsolete and can be as risky as having no plans at all(Savage, 2002).

Changes in personnel, technology, infrastructure and environment alter written procedures in some way. Consequently, testing is conducted to ensure proper documentation and maintenance (Hawkins, Yen et al., 2000).

Testing the plan is an on-going activity which is essential to ensure reliability. The Business Continuity and Disaster Recovery plan should be exercised at least annually. Furthermore, selected area reviews of the plan may be conducted on an as-needed basis(Iyar and Bandyopadhyay,2000)

Testing is used to determine whether all the individual contingency plans are adequately written to ensure continuity of business processes and the recovery of the data centre (Botha and Von Solms, 2004).

Testing's purpose is ensuring that documented contingency procedures are regularly evaluated and modified by proper recovery personnel (Karakasidis, 1997). This process is undertaken to confirm that all required personnel skills are updated and that all resources are aware of their responsibilities. To affirm completeness, accuracy and reliability of the Business Continuity and Disaster Recovery program, a series of test programs should be developed and conducted (Heikkinen and Sarkis, 1996; Payne, 1999; (Cerullo and Cerullo, 2004).

There are numerous reasons for testing the plan. The obvious reason is to make sure that the plan will work in the event of a real disruption or disaster. However, the underlying reasons that testing helps the plan work more effectively is that testing serves these purposes (Snedaker, 2007):

- Checks for understanding of processes, procedures, and steps by those who must implement the plan.

- Validates the integration of tasks across the various business units and management functions.
- Confirms the steps developed for each phase of the plan's implementation.
- Determines whether the right resources have been identified.
- Familiarizes all involved parties with the overall process and flow of information.
- Identifies gaps or weaknesses in the plan.
- Determines cost and feasibility.

2.7.6.2. Business Continuity and Disaster Recovery Plan auditing

2.7.6.2.1. Approaches to test/audit

Approaches to test/audit include (Savage, 2002):

- The use of specialist consultants.
- Working through templates and checklists.
- The use of an in-house test/audit team, with some specific training.
- And simple "brainstorming" of the plan by key personnel, via intensive meetings and workshops.

2.7.6.2.2. Performing information technology Systems and Security Audits

By definition, an audit is the systematic examination against defined criteria. If the company is required to comply with laws or regulations, it has no doubt been through rigorous audits. The audits performed to conform to these regulations may help in Business Continuity and Disaster Recovery planning and may need to be included in the plan (Snedaker, 2007).

2.7.6.2.3. information technology Systems and Security Audits

With respect to Business Continuity and Disaster Recovery planning, systems auditing should include several key elements. These include (Snedaker, 2007):

- Ensuring information technology risk mitigation strategies are in place and properly implemented/configured.
- Ensuring systems identified by the Business Continuity and Disaster Recovery plan are still in place and functioning.
- Identifying areas where new technology has been implemented and may not be incorporated into the Business Continuity and Disaster Recovery plan.

- Identifying areas where technology has been retired or modified, resulting in the need to revise the Business Continuity and Disaster Recovery plan.
- Reviewing the processes identified in the Business Continuity and Disaster Recovery plan with respect to information technology systems to ensure the steps and processes are still correct, complete, and relevant.
- Verifying that the information technology incident response team is in tact and has a clear understanding of roles, responsibilities and how to implement the information technology-specific segments of the Business Continuity and Disaster Recovery plan.
- Reviewing data regarding various systems to ensure they are still compliant with the Business Continuity and Disaster Recovery plans. These systems include operating systems, networking and telecommunications equipment, database and applications, systems backups, security controls, integration, and testing. Any of these areas is subject to frequent change. An audit can help assure the Business Continuity and Disaster Recovery plan will still work if implemented.

2.7.6.3. Business Continuity and Disaster Recovery Plan Maintenance

2.7.6.3.1. Plan Maintenance Activities

The success of a Business Continuity and Disaster Recovery plan depends on how often the plan is exercised, how regularly the plan audits are conducted, and how often the plan is updated and maintained to conform to changes in the organization itself (Iyar and Bandyopadhyay, 2000).

The plan would become outdated when new applications or changes of business strategy are introduced. Therefore, the plan should be updated to reflect the changes (Chow, 2000), this is done to ensure that the plan stays effective and up to date (Botha and Von Solms, 2004).

As Business Continuity and Disaster Recovery plans should be tested on a regular and periodic basis, they should likewise be maintained to the same effect. Changes in technology (hardware and/or software), personnel, business strategy and the environment necessitate continuous updates of the Business Continuity and Disaster Recovery plan. (Arend, 1994; Paradine, 1995; Carvajal-Vion and Garcia-Menendez, 2003).

This last phase of the Business Continuity and Disaster Recovery program cycle ensures that the previous completed steps remain as updated as possible (Brabara, 2006).

There are a number of activities beyond change management that can help the planner to keep his plan up to date and ready to go, this is a sample list of such activities(Snedaker, 2007):-

1. If the plan is revised, the Business Continuity and Disaster Recovery team members (or those who should have the latest copy of the plan) should be notified in a timely manner.

2. The plan should use a revision numbering system so team members know whether they have the latest version of the plan.

3. Review, update, and revise key contact information regularly. This includes staff, vendors, contractors, key customers, alternate sites and facilities, among others.

4. Create a Business Continuity and Disaster Recovery plan distribution list that is limited to authorized personnel but that includes all relevant parties. This distribution list should include off-site and remote facilities that may be used in the event of Business Continuity and Disaster Recovery plan activation.

5. Be sure there are up-to-date copies of the Business Continuity and Disaster Recovery plan off-site in the event the building is inaccessible.

6. Be sure there are up-to-date paper copies of the Business Continuity and Disaster Recovery plan on-site in the event information technology systems go down.

7. Implement a process whereby all old versions of the plan are destroyed or archived and new versions replace them. This helps avoid a scenario where team members are working from different versions of the plan.

8. Always check soft copy and remote storage copies of your plan when changes are made to the plan. If you store copies off-site or at your alternate work site, these versions should be updated any time the plan is modified.

9. Whenever significant changes are requested or implemented, test the plan. This will ensure there are no new areas of concern and will help train staff on the changes.

10. Integrate Business Continuity and Disaster Recovery considerations into operational processes to reduce plan maintenance efforts in the future.

11. Assign responsibility for managing Business Continuity and Disaster Recovery change notification and requests to someone on the Business Continuity and Disaster Recovery team. The project management adage that a task without an owner won’t get done is especially true here.

12. Document plan maintenance procedures and follow these procedures to avoid introducing additional risk into the project.

13. Incorporate training into the change process so changes to people, process, technology that are incorporated into the Business Continuity and Disaster Recovery plan also trigger changes to training plans.

14. Be sure to include Business Continuity and Disaster Recovery plan testing, training, auditing, and maintenance activities in your information technology or corporate budget for future activities related to business continuity and disaster recovery.

2.7.7. Training for business continuity and disaster recovery

Recovery team members must clearly understand their responsibilities and must be adequately trained beforehand to ensure smooth and quick implementation of the Business Continuity and Disaster Recovery pan. The key personnel to carry out the procedures must be adequately trained and kept up to date as the procedures have changed (Chow, 2000).

People need to be trained before they are tested in any particular skill. If you run a test of a highly complex skill before a person has had a chance to practice it, you are highly likely to find that the person fails the test(Morwood,1998)

Hence, training is a crucial element within the development stages of implementing the Business Continuity and Disaster Recovery program (Cerullo and Cerullo, 2004) and should be part of the Business Continuity and Disaster Recovery framework. Personnel need to be kept up-to-date on the latest developments within the Business Continuity and Disaster Recovery plan. It is incumbent upon management to train all affected recovery personnel regarding all Business Continuity and Disaster Recovery procedures (Paton, 1999; Lee and Ross, 1995).

Business continuity training must form part of the organization's training framework and should be allocated part of the training budget. The training should be carried out as soon as the plan is complete as well as when it undergoes significant changes (Botha and Von Solms, 2004).

Disaster recovery and business continuity training includes defining the scope and objectives for the training, performing needs assessment (gap analysis), developing training, scheduling and delivering training, and monitoring/measuring training(Snedaker, 2007).

2.7.7.1. Training Components

2.7.7.1.1. Training Scope, Objectives, Timelines, and Requirements

Ideally, the planner should develop a training project plan that ties in with the Business Continuity and Disaster Recovery project plan. The training plan should include a statement of scope as well as a list of high-level objectives. These objectives might be parsed out to include objectives for each of the implementer groups. In addition, the timelines for training various teams should be developed. Keep in mind that some people may be members of more than one team, so training and training subjects should take that into consideration. Then, develop requirements for training. One of the easiest ways to make sure training meets its stated objectives is to clearly define the objectives, then list the requirements to meet those objectives (Snedaker, 2007).

2.7.7.1.2. Performing Training Needs Assessment

The needs assessment phase is essentially a gap analysis. The planner should review current skill sets against required expertise to carry out various functions and determine what sort of training would best fill the gap. In many cases, training needs become evident during the testing of the plan. As he tests his plan, he will see areas where specialized or updated skills and knowledge will be required to successfully execute the plan. He can make note of these potential skill gaps during his plan testing and circle back to include these in his training plans (Snedaker, 2007).

2.7.7.1.3. Developing Training

Many companies have limited time or funds available for training, much less for Business Continuity and Disaster Recovery training. However, many studies support the thought that companies that train their employees benefit not only from improved productivity but greater loyalty as well. Targeted training to maintain or improve skills, especially those related to mission-critical business functions, can be accomplished relatively quickly and often at a reasonable cost. As with other risk factors in Business Continuity and Disaster Recovery planning, the risk of having untrained personnel can easily be mitigated through training, and it may also help drive productivity within the organization (Snedaker, 2007).

2.7.7.1.4. Scheduling and Delivering Training

Scheduling and delivering training is a secondary challenge after getting the training budget approved. These days, the planner can often find various training programs online that people can attend on their own schedule. If he uses a flexible online learning system, he has to be sure to set timelines and test for knowledge along the way.

2.7.7.1.5. Monitoring and Measuring Training

The first step in monitoring and measuring training is the development of clear objectives and outcomes for the training. If you don't know what should be accomplished in training, you won't be able to determine if the training was effective (Snedaker, 2007).

Monitoring also involves ensuring key personnel have actually attended required training and have not somehow accidentally fallen through the cracks. If staff members leave or move into different positions, replacements need to be trained, so the planner need to develop some method of periodically checking his key Business Continuity and Disaster Recovery staff positions and ensure individuals are still in place and ready to perform their assigned Business Continuity and Disaster Recovery duties. These vary widely from one company to the next. He

may be able to work with his HR department if they have an established system for tracking employee training and certification in place (Snedaker, 2007).

2.8 Study Model

After reviewing the literature, this model is suggested in this study, which was extracted from DRII and BCI professional business continuity models.

Business continuity and disaster recovery plan consists of the following components.

- Project Initiation.
- Risk Assessment.
- Business Impact Analysis.
- Strategy Development.
- Business Continuity/Disaster Recovery Plan Development.
- Continuity and Disaster Recovery Plan Testing, Auditing, and Maintenance.
- Training for business continuity and disaster recovery.

Chapter Three:

Overview of Palestine Securities Exchange Listed Companies, and Information Technology

Preface:

This chapter gives an overview at the Palestinian security exchange and it's listed companies, and the calculation of Al-Quds index.

This is in addition to reviewing the basic elements of information systems, its major types, the served groups, and how it impacts the business firms, this is beside reviewing the information technology departments and services performed by them.

3.1. Introduction to Palestine Securities Exchange

At the early beginning of 1995, a group of pioneers in the Palestinian private sector felt the necessity of establishing a well-regulated and up-to date market for securities in Palestine. The main goal was to tap and channel both domestic and foreign capital into the business community through long-term financing of commercial and infrastructure projects. Their ideas shaped into an agreement signed on the seventh of November 1996 with the Palestinian national authority to launch the Palestine securities exchange as a private shareholding company. The Palestine securities exchange conducted its first trading session as the first fully automated and electronic Arab stock exchange on February 18, 1997. Despite its modest beginning, the exchange maintained continued growth in terms of listed companies, number of sessions and trading volumes. They have started with a few listed companies in 1997, increasingly the number of listed companies rose to 36 in 2007. A further growth is being expected in the future (PSE, 2008).

3.1.1. Listing Conditions

Listing of shareholding companies is of two levels: First Market and Second Market. Listing conditions of these two markets are different. Following are the requirements for listing each of them:

First Market listing conditions:

Listing conditions of the shareholding companies stocks on the First Market include:

- The subscribed capital of the company shall not be less than 2,000,000 (two millions) Jordanian Dinars and shall be fully paid.
- The number of the company's shareholders shall not be less than 150 shareholders.
- The share of the public shareholders (Free Float) in the company's subscribed capital shall not be less than 25%.
- The number of issued shares shall not be less than hundred thousand (100,000) shares.

- The company shall have actually started its activities, published its financial statement for at least two fiscal years, which are prepared in accordance with the International Accounting Standards, and gained net profits of not less than 5% of the paid capital before tax during the fiscal year that preceded the submission of the Listing request. As regards the newly established companies, such companies shall provide feasibility studies for the coming two years.
- The constitutional board or the general assembly of the company shall prove to convene at least once a year or/and the company shall pledge that.
- Members of the company's board of directors shall have demonstrated expertise of such company's business field, or such company has engaged in an agreement with a specialized and expert consultant in such company's field of activities.

Second Market listing conditions:

Listing conditions of the shareholding companies stocks on the Second Market include:

- The subscribed capital of the company shall be fully paid.
- The share of the public shareholders (Free Float) in the company's subscribed capital shall not be less than 25%.
- The company shall have published its financial statements for at least one fiscal year prepared in accordance with the International Accounting Standards and the company shall pledge to publish its balance sheet and its works results in the local dailies before trading its stocks at the Exchange. As to newly established companies, such companies shall provide economic feasibility study.
- The constitutional board or the general assembly of the company shall prove to convene at least once a year or/and the company shall pledge that.
- The number of shareholders shall not be less than (50) shareholders.

3.1.2. Al-Quds index

The base date for the Al-Quds index is July 8, 1997 = 100 points; at that time (10) symbols were chosen to represent all sectors in the market and also the most liquid symbols.

In 2007 Palestine Securities Exchange has raised the number of symbols in Al-Quds index to (12) symbols; this decision was taken to reflect the increase in listed companies at Palestine Securities Exchange (33 company at the end of 2006).

- Each year this sample of symbols is edited according to the statistics of that year.
- The below table shows the symbols included in Al-Quds index for the year 2007:

Table 3.1: Symbols of companies included in Al-Quds index

#	Symbol	Sector
1.	PALTEL	Service
2.	PEC	
3.	PADICO	Investment
4.	PRICO	
5.	PIIC	
6.	AIG	Insurance
7.	NIC	
8.	AIB	Banking
9.	BOP	
10.	BPC	Industry
11.	JCC	
12.	GMC	

(Adopted from PSEI 2008 Table, Symbols of companies included in Al-Quds index, Available at ((http://212.14.224.121/PSEWEB/Forms/en/IndexAlQuds.aspx))(Accessed at 6 Dec,2008).

3.2. Palestinian Listed Companies

The number of listed companies in period of the research was 38, these companies were distributed in 5 main sectors.

The main sectors were as the following:

- Service sector.
- Industry sector.
- Banking sector.
- Insurance sector.
- Investment sector.

The following table clarifies the distribution of Palestinian listed companies over the five main sectors.

Table 3.2: Companies distribution over their sectors.

Sector	Company Name	Trading Symbol	Established Date	Listing Date
Service	Arab Hotels	AHC	1996	1998
	Arab Real Estate Establishment	ARE	1986	1997
	Grand Park Hotel & Resorts	HOTEL	1999	1999
	Nablus Surgical Center	NSC	1995	2008
	Palestine Telecommunications	PALTEL	1995	1997
	Palestine Electricity Company	PEC	1999	2004
	Arab Palestinian Shopping Centers	PLAZA	1999	2000
	The Palestinian Company for Distribution & Logistics Services	WASSEL	2005	2007
Industry	Arab Concrete Products	ACPC	1978	1999
	Arab Company for Paint Products	APC	1990	1997
	Palestine Poultry	AZIZA	1997	2004
	Birzeit Pharmaceuticals	BPC	1973	2004
	Golden Wheat Mills	GMC	1995	2005
	Jerusalem Cigarette	JCC	1964	1997
	Jerusalem Pharmaceutical	JPH	1969	1997
	Palestine Plastic Industrial	LADAEN	1998	2002
	The National Carton Industry	NCI	1993	2006
	The Vegetable Oil Industries	VOIC	1953	1999
Banking	Arab Islamic Bank	AIB	1995	1997
	Alrafah Microfainance Bank	AMB	2005	2007
	Bank Of Palestine	BOP	1960	2005
	Palestine Commercial Bank	PCB	1992	2006
	Palestine Investment Bank	PIBC	1994	1997
	Al-Quds Bank	QUDS	1995	1997
	Palestinian Islamic Bank	ISBK		2009
Insurance	Arab Insurance Establishment	AIE	1975	1997
	Ahliea Insurance Group	AIG	1994	1997
	AL-Mashreq Insurance	MIC	1992	2006
	National Insurance	NIC	1992	1997
	Trust International Insurance	TRUST	1995	2008
	Arab Investors	ARAB	1997	1997
Investment	AlTiman for Investment & Development	IID	2004	2006
	Jerusalem Real Estate Investment	JREI	1996	2006
	Palestine Development & Investment	PADICO	1993	1996
	Palestine Investment & Development	PID	1993	2006
	Palestine Industrial Investment	PIIC	1995	2002
	The Palestine Real Estate Investment	PRICO	1994	1997
	Union Construction & Investment	UCI	2005	2007

3.3. Information System

An information system can be defined technically as a set of interrelated components that collect (or retrieve), process, store, and distribute information to support decision making and control in an organization. In addition to supporting decision making, coordination, and control, information systems may also help managers and workers analyze problems, visualize complex subjects, and create new products (Laudon and others, 2006).

An Information System is the system of persons, data records and activities that process the data and information in a given organization, including manual processes or automated processes. Usually the term is used erroneously as a synonym for computer-based information systems, which is only the Information technologies component of an Information System. The computer-based information systems are the field of study for Information technologies however these should hardly be treated apart from the bigger Information System that they are always involved in(Wikipedia, 2008).

Information systems contain information about significant people, places, and things within the organization or in the environment surrounding it. By information we mean data that have been shaped into a form that is meaningful and useful to human beings. Data, in contrast, are streams of raw facts representing events occurring in organizations or the physical environment before they have been organized and arranged into a form that people can understand and use (Laudon and others, 2006).

Three activities in an information system produce the information that organizations need to make decisions, control operations, analyze problems, and create new products or services. These activities are input, processing, and output. Input captures or collects raw data from within the organization or from its external environment. Processing converts this raw input into a more meaningful form. Output transfers the processed information to the people who will use it or to the activities for which it will be used. Information systems also require feedback, which is output that is returned to appropriate members of the organization to help them evaluate or correct the input stage(Laudon and others, 2006)..

Although computer-based information systems use computer technology to process raw data into meaningful information, there is a sharp distinction between a computer and a computer program on the one hand, and an information system on the other. Electronic

computers and related software programs are the technical foundation, the tools and materials, of modern information systems. Computers provide the equipment for storing and processing information. Computer programs, or software, are sets of operating instructions that direct and control computer processing. Knowing how computers and computer programs work is important in designing solutions to organizational problems, but computers are only part of an information system (Laudon and others, 2006).

Information Technology, as defined by the Information Technology Association of America, is "the study, design, development, implementation, support or management of computer-based information systems, particularly software applications and computer hardware." information technology deals with the use of electronic computers and computer software to convert, store, protect, process, transmit, and securely retrieve information(Wikipedia,2008).

Information Technology also known as Information and Communication(s) Technology and Info-comm (in Asia) is concerned with the use of technology in managing and processing information, especially in large organizations. In particular, information technology deals with the use of electronic computers and computer software to convert, store, protect, process, transmit, and retrieve information.

The information technology department of a large company would be responsible for storing information, protecting information, processing the information, transmitting the information as necessary, and later retrieving information as necessary(Laura Schneider,2008).

3.4. I.T. Department

3.4.1. Department

Departments are the entities organizations form to organize people, reporting relationships, and work in a way that best supports the accomplishment of the organization's goals. Departments are usually organized by functions such as human resources, marketing, administration, sales, and information technology. Departments are usually led by a Manager, a Supervisor, a Director, or a Vice President according to department size and importance.

3.4.2. I.T. Department

As the use of electronic communication has become more common for businesses of all sizes, so has the need for the creation and staffing of information technology departments in any company that employs telephony and Internet devices to conduct business. Here is some basic information on the information technology department, and how it may function as both a creative and a practical part of any business operation (Tatum, 2009).

Essentially, the information technology department is a collection of persons who are experts when it comes to electronic communications of all kinds. In addition to understanding what forms of electronic data, visual, and audio communication are available, the information technology department will be able to evaluate available services and determine which services and vendors can provide the best equipment and service support for the company. Along with making determinations about what equipment to use and which vendors to work with, the information technology department will also oversee the day to day operations of all electronic communication devices within the company (Tatum, 2009).

Oversight of all equipment would include configuring network access, setting up and making changes to existing workstations, and assigning access rights at various levels to key personnel within the company. The competent information technology tech would also ensure there is a workable disaster recovery backup in the event that some section of the network should happen to fail. The best information technology department teams understand the importance of network redundancy to the continued healthy operations of the company (Tatum, 2009).

In many companies, the final decision with selection of conference call vendors, web site hosting, choice of primary and backup servers, and even the choice of a local and long distance phone service provider will rest within the information technology department. With an eye to making sure the company has the best communication resources on hand that it can afford, the information technology department is much more than just a group of people who show up when your computer crashes. The information

technology department plays a valuable role in making all other departments productive and successful in their endeavors (Tatum, 2009).

Chapter Four:
Previous Studies

Preface:

This chapter reviews the previous studies conducted in business continuity and disaster recovery planning.

Many aspects in business continuity and disaster recovery planning had researched, and here are the significant studies which related to this research.

In essence this is the first study to cover this area of research as no researches were made in regard to business continuity and disaster recovery planning in Palestinian companies, and no similar Arabic research has been found in such field.

4.1. Previous Studies

1. "Information technology disaster recovery: Oman and Cyclone Gonu lessons learned"(Al-Badi and Others, 2009)

This paper aimed to explore the issues of information technology disaster recovery and business continuity planning in light of Cyclone Gonu in Oman.

The paper included a survey public and private sector organizations together with their disaster recovery and business continuity planning practices.

The paper investigated how public and private organizations in Oman plan to respond to disasters. It showed that while some organizations pay attention to the need for disaster recovery and business continuity planning, many do not. A significant finding is that while organizations have disaster related plans, almost half of those surveyed do not rehearse them. Nevertheless, organizations surveyed indicate that they have learned valuable lessons from Gonu. It remains to be seen whether these lessons will be turned into effective and properly deployed disaster recovery and business continuity plans.

This paper draws lessons from the experiences and challenges raised by Gonu, and concludes with a set of recommendations that organizations may adopt to ensure business continuity. It provides a useful evaluation of the preparedness of information technology departments in both public and private sectors in Oman. The recommendations given could be of a great value for many organizations and groups, spreading awareness of the importance of being prepared for such eventualities.

2. “Effectiveness of Information "Security Management at the Palestinian Information Technology Companies” (Taye,2008)

This study aimed to identify the extent of the effectiveness of Information Security Management in Palestinian Information Technology companies (Jerusalem, Westbank, and Gaza). To achieve this aim, the researcher investigated ten domains of information security management in forty one companies. The ten domains included the Information Security Policy, Organizational Security, Asset Classification and Control, Personnel Security, Physical and Environmental Security, Computer and Network Management, System Access Control, Systems Development and Maintenance, Business Continuity Planning, and Compliance.

The findings of the research showed that all domains except the Organizational Security were affecting the effectiveness of Information Security Management in Palestinian Information Technology companies.

Moreover, the study revealed that around two thirds of Palestinian information technology companies (68.3%) have a managed process for developing and maintaining business continuity throughout the organization, while other companies (7.3%) do not have such kind of process. And the events that could cause interruptions to business process are identified in less than two thirds of companies (61%), while other companies (12.2%) do not identify such kind of events. And less than two thirds of companies (63.4%) developed plans to restore business operations within required time frame following an interruption or failure to business process, while other companies (17%) do not develop such kind of plans.

The study revealed also that around two thirds of companies (65.9%) have a single framework of business continuity plan which is maintained to ensure that all plans are consistent and identify priorities for testing and maintenance, while other companies (19.5%) do not have such kind of framework. And little more than one halve of companies (56.1%) testing their business continuity plans regularly to ensure that they are up to date and effective, while other companies (14.6%) do not test their plans regularly.

This confirmed that the Business Continuity Planning in the Palestinian information technology companies affecting the effectiveness of Information Security Management in these companies to some extent.

3. "Business continuity, disaster recovery awareness high" (Lumpur,2007)

The purpose of this study is to explore the awareness of importance of Business Continuity and Disaster Recovery in Malaysian organizations. The survey of this study had 53 respondents who were information technology and decision makers in their organizations in both the private and public sector. The analysis of the study reveals that most of the respondents are employing local providers to implement their business continuity and disaster recovery plans, with 34% employing foreign providers to build the infrastructure and plan for the companies. Spending on business continuity and disaster recovery will continue to be driven by medium-sized to large enterprises.

Here are some of the survey's interesting results:

1. Most of the companies prefer both onsite and secondary disaster recovery environments.
2. Almost 70% of respondents had undertaken a business impact analysis before embarking on any business continuity and disaster recovery infrastructure.
3. A majority of the respondents had their business continuity plans tested less than a year ago, with 40% testing business continuity and disaster recovery plans tested in the last six months.
4. 92% of respondents have a recovery time and point objective of 0 hours to 24 hours.
5. Large multinational companies tend to have less than three hours of recovery time and point objective.

4. "Business continuity: Preparation over Prevention"(Jackson,2006)

This paper reported that Business continuity encompasses keeping the business operational and efficient throughout many minor and perhaps more likely business disruptions. Such disruptions to be considered include failing information technology systems, maintenance of information technology systems, a workplace fire, stolen or damaged laptops, employee illness, public transport interruptions or accidents on a major motorway. Business continuity is being able to work from wherever and at whatever time one needs to do it. A business continuity interruption encompasses any major or minor interruption to a company's day-to-day business operations. By approaching business continuity as part and parcel of corporate planning, and installing a multi-departmental team to own the concept, businesses can design and roll out their technology and processes with an element of continuity built in.

The survey, which quizzed senior management on business continuity trends across Ireland, the UK, Germany, France, Italy and Spain, revealed that most Irish companies believe it would be bad practice not to have a business continuity plan. 70% of those surveyed believe that with no business continuity plan in place the effects of a major business continuity event on day-to-day operations would be catastrophic or at least very severe. In addition 59% said it would have a very severe effect on profits.

Encouragingly, these findings suggest that business continuity plans are higher up the value chain in Ireland than in Europe. However Irish companies need not be complacent with this fact. With 10% of Irish companies admitting to having suffered a major business continuity event within the past 3 years, business continuity plans are a crucial part of today's business structure. Irish companies need to be aware of the huge revenue loss and the effect on day-to-

day operations that they will face if their staff are simply unable to continue working because they can't reach the office, or because their information technology systems are being maintained, or have failed.

The study was based on 100 interviews with medium and large organizations in each country. Interviews were conducted at senior business management level with particular focus on information technology Directors and Managers.

The survey highlighted the necessary solutions that businesses should implement to ensure continuity including:

- server backups,
- web mail,
- remote/home working,
- server based computing, and
- Personal Digital Assistants.

5. "Determining the Critical Success Factors of an Effective Business Continuity / Disaster Recovery Program in a Post 9/11 World" (Barbara, 2006).

This research project aims to fulfill two key objectives. First, this project will examine whether the ranking of critical success factors for implementing a Business Continuity and Disaster Recovery program have changed from previous research, specifically subsequent to the events of September 11th, 2001 (9/11). Second, this study will attempt to further increase contribution to the academic and practitioner communities by outlining several critical success factors not referenced within previous research.

A multi-method approach was used in this research, a qualitative analysis of 11 interviews was conducted and contrasted to results carried out through a quantitative analysis of 52 respondents through a survey questionnaire. After careful analysis of quantitative and qualitative results, four sets of critical success factors were proposed and supported: Business Continuity and Disaster Recovery intrinsic factors, personnel requirements, analysis process and managerial issues.

Surprisingly, extrinsic factors, although still required in a Business Continuity and Disaster Recovery initiative, have lost the luster of the days when storage, applications and data

dominated over people and processes. In essence, it was shown that the propositions formulated were confirmed, partially or fully, regarding such issues as impacts stemming from 9/11, new critical success factors emanating since previous research and the aforementioned existence of a reduced set of critical success factors. The three factors were Effective communication, Service Level Agreement, and Business Continuity and Disaster Recovery Implantation Plan.

In addition, analyses comprised a quantitative review of the interviews, descriptive statistics and exploratory analysis using SPSS. Consequently, conclusions were derived between and within results from these types of analyses, implications to academics and practitioners suggested and future research proposed.

The exploratory factor analysis confirms a majority of the applicable propositions. Lending support to the third proposition, a new set of factors has emerged, classified under the headings of Business Continuity and Disaster Recovery intrinsic factors, personnel requirements, analysis process and managerial issues. Such a classification can be attributed to the events of 9/11 having shaken the contingency planning field and the practitioners that operate therein. Focus has shifted from applications, storage and data-based factors to resources-driven aspects as personnel and organizational priorities. It is therefore incumbent upon academics and practitioners alike to take advantage of this information, tailoring the Business Continuity and Disaster Recovery program to effectively handle these new factors.

The critical success factors according to Barbara model are:
CSFI Top Mgmt Commitment
CSF2 Adequate Financial Support
CSF3 Alignment Of disaster recovery planning Objectives with Company Goals
CSF4 Adoption of Project Management Techniques
CSF5 presence of formal recovery planning committee
CSF6 Participation of Representatives from Each Dept.
CSFI Engagement of External Consultant
CSF8 Risk Assessment & Impact Analysis
CSF9 Impact Analysis
CSF10 Determination of Maximum Allowable Is Downtime
CSF11 Priority of Information systems Applications
CSF12 Off-site Storage of Backup
CSF13 Presence of Emergency Response Procedures
CSF14 Training of Recovery Personnel
CSF15 Appropriate Backup Site
CSF16 Periodical Testing of disaster recovery planning
CSF17 Maintenance of disaster recovery planning
CSF18 Insurance Coverage For information system Loss

NEW CSFS

CSF19 Effective Communication
CSF20 Service Level Agreements
CSF21 Business continuity/Disaster Recovery Implementation Plan & Templates

6. "Disaster recovery and continuity planning for digital library systems" (Cervone, 2006)

The purpose of this paper is to provide an overview of disaster recovery and contingency planning for digital library systems.

The methodology used in this paper was best practices, the paper develops a context for developing business continuity and disaster recovery plans.

This paper found that, the business continuity planning and disaster recovery are important components of digital library system planning. Two out of five organizations that incur a major disaster event are unable to permanently recover, but by developing a continuity and recovery plan in advance, libraries can greatly increase the likelihood of long-term recovery of institutional resources.

The value of this paper will be of interest to systems developers and managers, as well as senior library management, who need to plan for unexpected organizational disruption. The paper provides a context and outline for developing a business continuity and disaster recovery plan.

In the end, a successful business continuity plan for the library will be based on two major criteria: how much is it worth to the organization and is it possible to really implement? In addition, the plan that is developed must be tested and kept current. If this is not the case, then changing organizational requirements may make the plan useless in the event of an emergency

7. "Strategic contingency planning" (Scott, 2006)

The objective of this study was to develop a strategic contingency planning model to be used to fully incorporate emergency management and business continuity into organization structures.

Presently, contingency planning is mainly done on an operational or tactical level. Current thinking suggests that contingency planning should be an active part of organizations.

This paper reported that a variety of business tools such as strategic planning and metrics can be adapted to help mature the contingency planning profession. Contingency planning processes are of strategic importance and, as such, need to fit into the organizational

structure more coherently. Organizations are facing greater challenges in an increasingly interconnected world, and contingency planning can help ensure the entity's operations continue. It is time for contingency planning to be an active part of an organization's overall strategic planning process. The organization will be better prepared for future disasters and crises.

8. **"Information systems for e-business continuance: a systems approach" (Bajgoric ,2005)**

This study seeks to address the continuity of the information systems for e-business, This study emphasizes that in today's e-business, system downtime is an unacceptable option since each hour, even minute of downtime may generate negative financial effects. In order to stay competitive, e-business must be continuous from a data availability perspective and agile with regard to data access. Therefore, there is a need for an information system which can support such a kind of business which will have high availability ratios. This study seeks to address this issue.

The paper presents a framework for the development of an e-business-oriented information system from business continuance perspective. It identifies high system availability and agile data access as two critical attributes in designing information systems for e-business. In addition, it identifies two sets of information technologies business continuity and business agility drivers that are crucial in developing such information systems. The presented framework can be used while selecting an appropriate operating platform, in order to achieve higher levels of continuous computing.

The result of this paper is a definition of conceptual framework for development of an information system for e-business. According to his model of a system consisting of five dimensions (objectives, environments, resources, components, management) an attempt is made to define an information system for e-business from business continuance perspective. In that sense, higher levels of system availability and agile data access are defined as major objectives of such systems. Technologies (resources) that can be used in achieving such levels are explained in the form of major information technology-drivers with some guidelines for selections of available technologies. These drivers have been defined as major technologies in boosting business continuity and enterprise-wide agility. Particularly, most widely used server platforms and server operating system are described in more detail with regard to their role in enhancing business continuity of contemporary e-business.

9. "A cyclic approach to business continuity planning"(Botha and Rossouw,2004)

This paper presents a complete business continuity planning methodology that should preferably be followed to ensure that such a plan is effective in protecting an organization and to ensure that an organization could recover after a disaster, and a complete business continuity plan should be in place. Such a methodology does not necessarily have to be different from those used in larger organizations. It does, however, need to be scalable. A large number of methodologies are available, but it is rarely specified how each should be implemented. Once again, smaller companies might have to implement a methodology differently than larger organizations. For this reason a method simplifying the implementation process was developed.

The approach followed was to define a business continuity planning methodology that is scalable to cater effectively for small to medium sized organizations. Furthermore, a cyclic implementation approach, utilizing four distinct cycles, was proposed. Each cycle concentrated on a specific business continuity planning goal and each goal was completed and tested before the next was started. With this implementation approach, an organization could implement only that part of a methodology that suits their unique recovery requirements.

A software prototype, implementing this cyclic approach has been developed and applied in a case study at a small organization. The results were very satisfactory and indicated that the methodology is indeed viable. Further development and implementation still needs to be conducted to really conclude what the real impact of this methodology would be in small to medium, as well as large organizations. A further paper might provide more detail on the viability and success of implementing this approach in a software product and conducting case studies in various organizations, varying from small to large.

10."Business continuity planning: a comprehensive approach" (Cerullom and Cerullo,2004)

This article presents a comprehensive approach to business continuity planning that seeks to mitigate against all major business interruptions of business systems. This article analyzes recent national and international surveys to develop insights about the current status of business continuity, including perceptions about internal and external information security threats.

This article provides guidelines for developing and improving a firm's business continuity planning, which has three components:

- Business impact analysis that takes into account a wide variety of potentially serious internal and external threats.
- Disaster contingency recovery plan.
- Training and testing component.

A large number of firms are minimizing the importance of testing and maintaining the business continuity planning, yet testing is critical to developing an effective business continuity planning and to assess the effectiveness of the business continuity planning before an actual disaster occurs.

11. "Business continuity planning as a facilities management tool" (Pitt and Goyal, 2004)

This paper highlights those organizations that do not plan in business continuity planning and those which focus on information technology rather than utilizing a holistic, integrated approach. Through extensive primary research this paper explores the current uptake and scope of business continuity planning within the business environment in the UK. The distribution of the questionnaire was to be restricted to the UK organizations of various sizes were selected at random from a UK business directory. In total 100 questionnaires were distributed, 50 sent to organizations from the manufacturing sector and 50 to a mixture of other market sectors. A total of 35 completed questionnaires were returned.

The paper shows that the viability and effectiveness of Business continuity planning is dependent on regular review, audit and testing.

The paper concludes that whilst many models of Business continuity planning exist the contents in most cases are unlikely to be generic and are more likely to be organization specific. As many variables exist that will influence the frequency of review, audit and testing, it is considered by the researcher that this field of Business continuity planning would merit separate investigation.

The results demonstrate also that approximately half of the respondents have fully integrated or comprehensive Business continuity planning . No causal links have been identified from other questions within the questionnaire, which supports the results. The results highlight that approximately two thirds of the Business continuity planning have been established for greater than five years.

12."An analysis of disruptions in the United States apparel manufacturing industry and identification of continuity planning strategies"(Deepak, 2003)

The purpose of this research is to conduct an exploratory analysis of the disruptions in the United States apparel manufacturing industry. The specific research objective is to identify and determine the nature of disruptions and the continuity strategies in the US apparel manufacturing industry. The research was conducted in two phases. The Phase I research gathered quantitative data using a three-page survey questionnaire developed by the researcher. The questionnaire was structured by a designated set of questions that were separated in relation to the disruptions and business continuity planning. The questions were structured to obtain an understanding of the types of business disruptions and the business continuity planning in the US apparel industry. The Phase II research gathered qualitative data from ten randomly selected US apparel companies. Data was gathered on the risk of disruptions and the response strategies used by companies to handle those risks. Companies were selected based on convenience sampling, as this study explores the current status of continuity planning in the industry to form the basis of future research. The risk of disruption to companies in apparel industry is significant due to the international nature of the business, large supply base, and the ever changing trade and customs regulations. The movement of the United States apparel manufacturing industry to low wage countries, increased use of independent and contract manufacturers and the trend towards full-package sourcing have increased the industry risk exposure. The business continuity planning culture is not well developed in the industry. Most companies studied have not completed their risk assessment and business impact analysis. The budget is not usually allocated for the development and implementation of continuity plans, and no training programs for employees were identified to effectively handle a disruption.

13. "Effective practices in business continuity planning for purchasing and supply management" (zsidisin and others,2003)

The purpose of this research was two fold; the first goal was to examine the current status of business continuity planning in supply management. Secondly, this study aimed to understand effective practices in business continuity planning for supply management with regard to processes, tools and techniques for risk assessment, and strategies and methodologies for managing supply risk.

The primary research method consisted of conducting case studies with firms that have established business continuity planning and risk management processes in supply

management.

An interview protocol was established before data collection and semi-structured interviews were conducted with key personnel from the case study firms. The interviewees comprised individuals with titles such as commodity manager, quality management specialist, vice-president of procurement, risk management specialist, supplier development liaison, risk manager, and others. Evidence of business continuity planning processes was also collected during the case studies in the form of documentation such as standard operating procedures, reports, and internal memorandums.

The case studies conducted to date have provided us initial insights for understanding these best practices. They have also reinforced the view that while risk cannot be ignored, it can be managed. Failure to manage supply chain risk can have devastating results. Effective business continuity planning is more than simply keeping critical data in more than one spot; it is a structured and formal process that identifies, manages, and reduces all forms and types of supply chain risks.

This study offers intriguing insights into this new development, it also demands more research. No firm that relies on the supply chain can afford to be without a business continuity planning. Yet, if firms and managers are to develop and implement effective and efficient business continuity planning, they need more insights into this system insights beyond the scope of this report.

14. "Higher Education Business Continuity Survey" (Greer,2003)

In this study, the author conducted an Internet survey to determine what effect, if any, the events of September 11, had on organizations contingency planning. He also wanted to identify any differences between the contingency planning processes for the higher education community and other organizations.

A survey was conducted of professionals in higher education institutions and in the industry at large to find differences in the contingency planning processes for these two types of organizations. The survey also asked the respondents if the events of September 11, 2001 had a lasting effect on their contingency planning processes.

The data from his survey revealed that almost a year after the disasters at the world Trade Center and the Pentagon, organizations had not responded to the degree expected at the

outset of the crisis, and the lasting effects of the terrorist attacks on September 11, 2001 will be felt for many years to come. The significance of those events cannot be overestimated in a multitude of areas. However, contingency planning was not dramatically affected by these events or more businesses would have implemented appropriate policies by the time this survey was taken.

The survey responses minimized the impact of the events of September 11, 2001 on contingency planning. A number of organizations updated their plan information, but did so as part of their normal contingency planning processes.

The survey also showed how organizations in higher education are lagging behind other organizations in adopting the most complete contingency plans. Due to the following factors, a college or university is no less at risk than a normal business would be from a disaster that caused a telecommunications failure:

- Distance learning programs
- On-line access to education materials
- Student registration over the Internet
- Heavy reliance on E-mail

15. "Disaster-preparedness of health maintenance organizations" (Bandyopadhya , 2002)

This paper discussed disaster recovery in Health maintenance organizations, Health maintenance organizations are becoming increasingly dependent on health management information systems for their effective functioning. Because of this reliance, Health maintenance organizations must use disaster recovery planning to safeguard their health management information system assets from natural as well as man-made disasters.

This article assesses the health management information system environment, and identifies the state of practice by Health maintenance organizations as it pertains to health management information system disaster preparedness.

Survey questionnaires were sent to 727 Health maintenance organizations across the USA from a list of Health maintenance organizations published by the American Hospital Association Guide to collect data pertaining to the following major themes:

- Health management information system dependence.
- Health management information system disaster preparedness.
- Types of computer facility.

- Dependence of Health maintenance organizations on health management information system.
- Health management information system downtime.
- Business impact analysis.
- Disaster recovery strategies.
- Disaster recovery planning testing.

The results indicated that 114 out of 121 (94.2 percent) Health maintenance organizations in the sample were either heavily or totally dependent on health management information system These facts and figures about the reliance of health management information system on Health maintenance organizations can help harried business executives to become more aware of the dependence of Health maintenance organizations on reliable functioning of health management information system.

The study indicated that only 65 out of 121 Health maintenance organizations (53.72 percent) completed business impact analysis. A major component of the business impact analysis is the gathering of data and documentation germane to the various functional areas of a health maintenance organization, and their needs with respect to health management information system

The results indicated that out of 65 Health maintenance organizations that conducted business impact analysis, 62 (95.38 percent) decided to develop a plan; whereas out of 56 Health maintenance organizations that did not complete business impact analysis, only 36 (64.28 percent) decided to develop a plan. Also, out of 65 Health maintenance organizations that conducted business impact analysis, only ten did not implement Disaster recovery planning (15.38 percent).

The results showed that out of 121 Health maintenance organizations, 98 (81 percent) decided to develop a plan. Out of 98 Health maintenance organizations, however, only 44 are applying disaster recovery planning regularly.

16. "A method for measuring the risk of e-business discontinuity" (Dalmadge, 2001)

This study focuses on measuring the risk of e-Business discontinuity. E-Business discontinuity is defined constitutively as a function of the availability accessibility of the business, and the quality of the business - customer interactions. An e-Business is deemed as having suffered a discontinuity if it becomes unavailable or

inaccessible to its customers or if it fails to provide satisfactory business customer interactions. Further, the factors influencing the causation of e-Business discontinuity are studied.

Causation is been studied here in terms of the factors that individually or collectively increase the risk of e-Business discontinuity. These are categorized as the "risk factors of e-Business discontinuity". Risk factors are categorized along two axes: based on the location of the problem and its contribution to the process of causation of e-Business discontinuity. Risk factors may be located within the information systems, the organization or its external environment. These risk factors affect causation in three ways: they trigger discontinuities, they enhance and suppress the triggers of discontinuity, and they influence the development of enhancers and suppressors of discontinuity.

Drawing upon interviews with e-Businesses/business continuity consultants and practitioners, anecdotal information and archival data a model was developed measuring the risk of e-Business discontinuity.

The findings suggest that the risk of e-Business discontinuity may be quantified based on the characteristics of the e-Businesses and its environment, which described here as risk factors. Further, a second set of factors is identified, capable of mitigating the impacts of an e-Business discontinuity. These are refereed to as moderating factors.

Three types of risk factors are identified: systemic, organizational and environmental. They are capable of individually or collectively influencing the risk of e-Business discontinuity. Moderating factors are associated with the nature of the e-Business, the nature of the industry in which it operates, the type of products it handles, and the nature of the trigger. Together the presence of risk factors and moderating factors determine the vulnerability of an e-Business.

17. "The role of business impact analysis and testing in disaster recovery planning by health maintenance organizations" (Bandyopadhyay, 2001)

In this article the author has illustrated the dependence of Health maintenance organizations on the reliable functioning of health management information system and the consequent need for disaster recovery planning to safeguard the health management information system environment. The study shows that Health maintenance organizations that conduct a business impact analysis are more likely to test disaster recovery plans, and Health maintenance organizations that test their plans are more inclined to implement them successfully. The results also indicate that, of 121 Health maintenance organizations that

responded to the survey, only 45 (37 percent) have actually implemented a Disaster recovery planning to protect their health management information system environment from possible disaster, showing that a majority of Health maintenance organizations do not currently have adequate protection. The author hope the facts outlined in this article will awaken managers to the importance of conducting a business impact analysis to assess the effect of a possible health management information system breakdown and of testing a Disaster recovery planning to ensure its effectiveness and reliability before implementation. These actions will enable Health maintenance organizations to better prepare for any possible information systems disaster and ready them to face the aftermath.

Of the 98 Health maintenance organizations that decided to develop Disaster recovery plannings, 46 percent, almost half never tested their plans. It reflects any changes made in operations, vendors, recovery strategies, procedures, and personnel information since the time the plan was last updated. Testing also refreshes the memories of all team members about the recovery process. Thus the likelihood of the proper implementation of a Disaster recovery planning increases substantially if it is tested.

The author collected data as part of a larger study via questionnaires that the author mailed to 727 Health maintenance organizations across the United States, which the author chose from a list published by the American Hospital Association Guide. The author requested that the questionnaire be filled out by the disaster recovery planner, management information system director, chief information officer, or some other key employee in the health maintenance organization who was involved in business impact analysis and disaster recovery planning.

The results of the study have several managerial implications for the implementation of disaster recovery planning by Health maintenance organizations. The study provides management with insights into the following critical issues faced by Health maintenance organizations today: (1) Are Health maintenance organizations sufficiently aware of their dependence on the reliable functioning of health management information system? (2) Are Health maintenance organizations aware of the potential danger that the adverse effects of a disaster can inflict on them? and (3) Are Health maintenance organizations protecting themselves in advance so that they can recover from a disaster with their critical applications running?

The study results indicated that 114 out of the 121 Health maintenance organizations in the sample (94.2 percent) were either heavily or totally dependent on health management information system In other words, 94 percent of Health maintenance organizations would either go out of business soon or run only with severe difficulty in the event of complete loss of support from. Also, 26.8 percent of Health maintenance organizations could withstand the loss of health management information system support for only up to 24 hours, and as many as 79.5 percent of Health maintenance organizations would be in critical condition if the outage should last for five days. These figures can help health maintenance organization executives to become more aware of their organization's dependence on the reliable functioning of health management information system Only 65 out of 121 Health maintenance organizations (53.72 percent) completed a business impact analysis. Out of those 65, 42 (64.6 percent) decided to test a disaster recovery plan, whereas of the 56 Health maintenance organizations that did not conduct a business impact analysis, only 12 (21.4 percent) decided to test such a plan. That clearly points toward the fact that Health maintenance organizations that conducted a business impact analysis were more aware of the impact of the potential unavailability of health management information system on the entire organization and its environment. These findings should persuade health maintenance organization managers to conduct a business impact analysis. Without it, managers will not comprehend the degree to which their organizations rely on health management information system, the risks associated with disasters, and the vulnerability of their organizations to these risks. Understanding the impact of an health management information system breakdown should alert management to the risks, which in turn will kindle interest in protecting their health management information system environment. Health maintenance organizations that implement disaster recovery plans are able to protect themselves against health management information system disasters better than those that do not. Effective functioning of a Disaster recovery planning depends on its periodic testing; thus testing facilitates the process of Disaster recovery planning implementation. The study indicated that out of 54 Health maintenance organizations that tested a Disaster recovery planning, 39 (72 percent) implemented it. Only six Health maintenance organizations implemented a disaster recovery plan without testing it. Therefore, it is important to stress that the chances of implementing a Disaster recovery planning successfully increase if it is tested periodically.

18. “Success factors for information system disaster recovery planning in Hong Kong” (Chow, 2000)

This paper identified the top five critical success factors for developing a disaster recovery planning Disaster recovery planning in information system. The paper compared the preferred pattern of Disaster recovery planning in four industries: namely banking, manufacturing, trading, and hotel. It was generally reviewed in this paper that the first three types of industries chose a similar set of priorities; however the hotel industry selects a different pattern because of its unique environment in our sampling. It is clear that other factors which did not fall into our selection criterion should also be considered when developing a Disaster recovery planning.

A structured questionnaire was used to collect data through direct mail. The sample for this study consisted of 400 companies from a cross-section of four industries: banking, hotel, trading, and manufacturing. A total of 98 completed questionnaires (i.e. 24.5 per cent) were returned. All of our respondents were the managers of Management Information System departments who were actively participating in Disaster recovery planning in their firms.

The critical success factors for disaster recovery planning are as the following:

1. Top management commitment
2. Adequate financial support
3. Alignment of disaster recovery planning objectives with company's goals
4. Adoption of project management techniques
5. Presence of a formal recovery planning committee
6. Participation of representatives from each department
7. Engagement of external consultant
8. Risk assessment and impact analysis
9. Determination of maximum allowable information system downtime
10. Prioritization of information system applications
11. Off-site storage of backup
12. Presence of emergency response procedures
13. Training of recovery personnel
14. Appropriate backup site
15. Periodical testing of disaster recovery planning
16. Maintenance of disaster recovery planning
17. Insurance coverage for information system loss

The top five critical success factors were reported as coherently meaningful and logical.

- Top management committee.
- Adequate financial support.
- Appropriate backup site.
- Off-site storage of backup.
- Training of recovery personnel.

For instance, the "top management support" is a crucial factor for the success of Disaster recovery planning for two reasons. First, it is a form of long-term planning because information is now a corporate asset for which the development of Disaster recovery planning for information system becomes a corporate-wide issue. Second, Disaster recovery planning involves an ongoing capital expenditure that may be in a form of acquisition of software, hardware, workplace, and/or manpower. Therefore, "adequate financial support" is a must. An additional requirement for launching the Disaster recovery planning in the findings is a safe location in which the valuable information should be kept so that it can be retrieved when needed. The two most common storage places are:

1 on-site location that is, information is kept within the company.

2 off-site location that is, information is kept at a place where the location does not inherit a similar environment condition as the present company.

The result showed that both of these storage places are considered as significant.

One note for the trading industry in Hong Kong is that their computer systems are mostly provided by and designed by a software house, which trains in-house recovery personnel. Although this is considered as significant, it is ranked as the fifth place.

19. "Disaster business continuity: promoting staff capability"(Paton,1999)

This paper discussed, from a human resource (HR) perspective, the implications of personal and group vulnerability, hazard and risk assessment, organizational systems, training and recovery management for disaster business continuity.

This paper reported that the object of business continuity planning is minimizing loss after a disaster. Achieving this goal requires that management and information systems are available to facilitate the recovery of core business operations as soon as possible. While safeguarding systems and/or arranging for substitutes is vital, it is equally important to ensure the availability of staff capable of operating these systems under adverse disaster conditions.

The discussion of this paper concluded that, while developing the administrative and technical resources required for disaster business continuity is important, ensuring the availability of staff capable of operating these systems is equally important. Given the difficulty in predicting the nature of the hazard likely to affect an organization, these issues should be considered within an all-hazards framework designed to facilitate an adaptable response capability. Information obtained from organizational analyses can be used to assist plan development, define the training and support needs of staff, and to develop systems and procedures that promote organizational resilience. Returning to productive capacity also requires that business continuity planning is a managed process which integrates staff and management systems via appropriately designed recovery resources. These integrated systems should be capable of adapting, over the course of the recovery period, to accommodate changing staff and business needs.

20. "Information technology contingency planning: management roles"(Ernest,1999)

This paper presents an analysis of selected participants in a survey of Australian organizations approaches to business and information technology contingency planning. In particular, it examines the role of management in planning and setting priorities for contingency planning, especially in those organizations that have specified that information technology is critical to the business operations.

The survey was undertaken because there was a perception that coping with disaster is a much-neglected aspect of management in Australia, and this analysis examines the underlying attitudes.

This paper examines in some detail the management attitudes and practices. In some organizations information technology has only a support role but the author wished to look at organizations for which some planning is essential. This paper therefore only reports on the responses in 27 organizations where the information technology has been assessed by the respondent to be critical. This selection is based on the response to the question: What is the maximum acceptable out-of-service time for your information technology services? This paper reports only on those responses that selected the shortest time frame - less than eight hours.

The questionnaire contained questions in the following categories: demographic, experienced contingencies, attitudes to planning, actual planning and backup procedures.

This paper has analyzed in some detail the attitudes of managers of 27 organizations, where information technology is critical to the business. Only five organizations have comprehensive continuity plans for information technology and the business, with three others having information technology plans. This very low level of preparedness is mirrored in their attitudes towards other corporate risk and security policies.

Responsibility for such matters is generally at too low a level in the organization and this does not appear to be likely to change in the near future.

The findings reveal that most organizations are inadequately prepared and fail to take the issue seriously. Business continuity is not rated as a high priority. Managers in the information technology area are also expected to take the responsibility for contingency planning for the whole business.

21. "Business continuity awareness and training programs" (Morwood, 1998)

This article emphasizes that business survival depends on the assured continuity of core business activities and supporting services. Business continuity plans are developed to provide this assurance, but the best laid plans can and often do go astray because the details of the plans are not effectively communicated to the people responsible for implementing them. There is no doubting the power of communication as a vital ingredient to success in all endeavors.

Also this article suggests that details of the Business continuity training program should be kept with the consolidated training material of the organization, rather than within the Business continuity plan documentation itself. This will ensure that Business continuity training receives appropriate priority within the organization's overall training schedule and that the focus on it does not die off six to twelve months after the initial development of the Business continuity plan.

A typical annual Business continuity training program would include:

- Quarterly awareness training sessions for newly recruited staff members or staff who have moved into positions with new responsibilities under the Business continuity plan.
- Quarterly call-out exercises.
- Bi-annual desk-top exercises.
- An annual operational exercise.

Details on staff members participating in each Business continuity training session and exercise, as well as copies of all reports generated by the exercises, should be recorded and stored within the organization's central training records.

These records can then be used to validate test results by confirming or otherwise whether staff members have received appropriate levels of training to enable them to perform at the required standard in tests of the Business continuity plan.

22. "Developing a Disaster Recovery Plan (Disaster recovery planning) Using a Data Base Package"(Sharon ,1998)

This paper discussed the procedures and techniques necessary to develop a disaster recovery for a database package on a microcomputer.

The paper reported that every organization must look at what the consequences of loss of their electric data processing resources could be. Three areas of exposure are: legal responsibility, financial loss, and business service. A critical part of the scope of Disaster recovery planning is to decide what level of service the Disaster recovery planning is designed to provide and what factors must be in place for the Disaster recovery planning to be implemented. The scope must be agreed to by the senior management of the firm prior to further progress on the plan.

There are six major priorities to create a Disaster recovery planning:

1. Conducting a risk analysis.
2. Developing emergency response procedures.
3. Establishing a vital records program.
4. Developing backup operations procedures.
5. Setting up recovery action procedures.
6. Establishing test plans.

The Disaster recovery planning is a dynamic system and should reflect the current status of the organization. Management should be kept aware of and involved in the Disaster recovery planning.

23. "Developing a suitable business continuity planning methodology" (Moh,1996)

This paper discussing the methodology used by a UK-based multinational banking group to develop its business continuity plans. The stages (modules) in the methodology are described sequentially.

The paper shows how this modularity is a key success factor, enabling a project manager to complete a module - with specific objectives, tasks and deliverables - within a specific time period, facilitating effective management of the overall project.

The paper suggests a methodology to develop suitable business continuity plan, including Project planning, Business impact analysis, Recovery strategy, Plan development, Testing.

24. "A project planning process for business continuity" (Kon, 1997)

This paper discusses the formulation of a business recovery plan. As a starting point, the business recovery timeline model is presented. This paper gives a framework of components to be considered in a business continuity project planning process, i.e. a risk reduction program. In the last few years disaster recovery practitioners for information technology systems and business recovery practitioners are constantly inundated with a vast array of contingency methods. One crucial element has surfaced: consider all risks when building a business recovery plan.

This paper reported that a business continuity project planning process comprises the following components and should be used in conjunction with a broad risk management program:

1-Obtain top management approval and support.

2-Establish business continuity planning committee.

3-Perform business impact analyses.

4-Evaluate critical needs and prioritize business requirements.

5-Determine the business continuity strategy and associated recovery process.

6-Prepare business continuity strategy and its implementation plan for executive management approval.

7-Prepare business recovery plan templates and utilities, finalize data collection then organize and develop the business recovery procedures.

8-Develop the testing criteria and procedures.

9-Test the business recovery process and evaluate test results.

10-Develop and review service level agreement(s).

11-Update and revise the business recovery procedures and templates.

25. "Critical elements of a disaster recovery and business/service continuity plan"(Pat,1995)

This research described how business functions/processes are identified and which level of business functions/processes is useful to investigate business impacts due to corporate crises in business area impact analysis.

Business area impact analysis is the foundation for developing corporate crisis management plans. An important problem of business area impact analysis is the lack of an analytical process to identify business functions/processes. Accordingly, it is difficult to determine which level of business function/process hierarchy decomposition related with business areas is used as a basis level to investigate business impacts. In order to carry out the business area impact analysis efficiently, it is first necessary to identify business functions/processes by the continued decomposition of the function/process hierarchy in the business areas with which the business deals. Second, which level of function/process hierarchy decomposition is used as a basis must be determined to investigate the financial impacts on business areas.

The survey is designed to gather some information about how the organization identifies business processes in order to analyze the business impacts due to various types of corporate crises. Of the nearly 120 contacted, 46 organizations agreed to respond and represented a sample spread across several key industries.

The survey asks for activities of business impact analysis conducted in organizations. It shows that 27 organizations (59 percent) conduct business area impact analysis, 17 organizations (37 percent) do not conduct it, and two organizations answer "do not know". Twelve organizations (71 percent) of 17 responders develop crisis management plan without business area impact analysis. Twenty-one organizations (78 percent) of 27 answers which conduct business area impact analysis are that vice-president is the highest level of executive involved in business impact analysis efforts. Only 16 organizations (59 percent) of 27 responders differentiate between business functions and business processes and eight organizations (30 percent) assume all of them as business processes. Thirteen responders (48 percent) of 27 organizations determine business functions and/or business processes by

manager's experience in each department or environment within his organization. Eight responders (30 percent) of 27 organizations identify business functions and/or business processes by conducting function/process hierarchy decomposition related with business areas. Only one responder selects business functions and/or business processes from computer based information systems. To investigate the financial and/or operational impacts on business functions/processes, top level functions (44 percent), or lowest level functions (7 percent), or top level processes (11 percent), or top level functions and top level processes (7 percent) are used as a basis level.

This survey indicates that most organizations do not have a structured approach to determine business functions and business processes as conducting business area impact analysis. The main problem is the lack of an analytical capability to identify business functions and business processes. Thus, it is difficult to determine which level of business function/process hierarchy decomposition related with business areas is used as a basis level to investigate business impacts.

Ideas are outlined in this article for a well-designed crisis plan applicable to many corporations, institutions, or government agencies. In the light of numerous community-wide disasters, as well as the singular disasters that corporations, institutions, municipalities and government agencies have suffered in the last few years, disaster recovery needs are detailed. Issues of site assessment such as whether or not a building is occupied, repairs, fire, and water cleanup, are discussed.

This study reported that the following issues have to be founded in business continuity plan.

- Emergency response plan.
- Emergency notification procedures.
- Emergency relocation procedures.
- Emergency access control and security.
- Emergency acquisitions and authorization.
- Emergency command centre requirements.
- Hot site-cold/site--warm site requirements.
- Asset management and retrieval.
- Product and distribution recovery.

- Vital records recovery.
- Telecommunications recovery.
- Electronics recovery/restoration.
- Hazardous contamination.
- Environmental compliance.

26. "Disaster recovery planning: Suggestions to top management and information systems managers"(Wong and others, 1994).

This paper suggests set of steps to develop a successful Disaster recovery planning.

- Obtain top management commitment.
- Establish a planning committee.
- Perform risk assessment and impact analysis.
- Prioritize recovery needs.
- Select recovery plan.
- Select vendor(s) and develop agreements.
- Develop and implement the plan.
- Test the plan.
- Continually test.
- Evaluate the plan.

The paper reported also that the successful development of a Disaster recovery planning depends not only on the proper implementation of the steps discussed above, but also on the involvement of top management. In particular, top management should:

- Provide adequate financial support.
- Communicate the policies, procedures, and standards of information system disaster recovery planning and implementation throughout the entire organization.
- Accept that implementation is the responsibility not only of the information system department, but of each functional department.
- Ensure that both internal and external auditors enforce standards for recovering information system.
- Understand that objectivity is critical to the success of a Disaster recovery planning.
- Recognize the stress level associated with the position of disaster recovery coordinators.

4.2. Comments on previous studies

After reviewing the previous studies, the following can be noticed:

- There are common steps in implementing the business continuity and disaster recovery plans.
- Business continuity and disaster recovery planning can affect information security management.
- Companies may have false sense of business continuity planning.
- International companies are highly interested in applying business continuity and disaster recovery planning, and managers believe that without such planning in place the effects of major events would be catastrophic or at least very severe.
- Business continuity and disaster recovery planning can be applied not only in information technology field but also in a lot of business functional fields.
- Business continuity and disaster recovery planning is mandatory in colleges and universities, because it are no less in risk that normal business, because of distance learning , online education documents, students inter net registrations, and the heavy reliance on e-mail.

But actually this study considered as the first study which applied in evaluating the business continuity and disaster recovery plans in Palestinian companies including all the components of the plan, to investigate to what extent the Palestinian companies are applying the business continuity and disaster recovery planning, and discovering the weaknesses in preparing and implementing these plans. This is in addition to find the relations between the components of the plan.

Chapter Five:
Research Methodology

Preface

This chapter aims at introducing a detailed presentation of methodology and procedures which were thoroughly adopted to conduct this study Evaluating Business continuity and Disaster recovery planning in information technology departments in Palestinian listed companies.

5.1. Research Design

The research aims to identify the reality of the usage of Business Continuity and Disaster Recovery planning in Palestinian companies.

The researcher used a modified model for achieving the research purpose, this model is a modified mixture between the suggested steps/components in DRII and BCI 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 the listed companies.

5.2. 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:

5.2.1 Secondary 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.

5.2.2 Primary 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 planning.

The third part consists of a set of forty six questions selected to measure the level of existence of the business continuity and disaster recovery components. Researchees were requested to fill the questionnaire through writing a number that ranges from 1 to 10 for each answer. Researchees 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 of managers or head of sections of information technology department in Palestinian companies, and then the input will be analyzed using the SPSS.

5.3. Research Population

This study will survey all of information technology managers or information technology head of sections or their deputies according to the organizational structure of the companies in the studied companies. A comprehensive survey was used in this study.

The number of companies which listed in Palestinian securities exchange in August 2009 was 38 company (when the sample chosen) and the research included all those companies in collecting the needed data. But there were four companies that did not respond to the questionnaire, and the researcher neglected 3 companies' responses because the respondents were not serious in answering questions due to that there was neither information technology department nor information technology service in those companies.

Two questionnaire were distributed to every company, 62 questionnaire from 31 companies were valid which shape about (81.6%) from the sample. On the other hand, questionnaires were distributed though telephone or email.

5.4. Validity and reliability of the questionnaire

The measurement has been applied on 30 companies 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 August 2009 and was collected in 2 weeks, and the all of these companies were involved in the final analysis.

5.4.1 Statistical analysis Tools

The researcher would use data analysis both qualitative and quantitative data analysis methods. The Data analysis will be made utilizing (SPSS 15). The researcher

would utilize the following statistical tools:

1) Cronbach's Alpha for Reliability Statistics

2) Spearman Rank correlation for Validity

3) Frequency and Descriptive analysis

4) Nonparametric Tests (Spearman correlation coefficient, Sign test, Mann-Whitney test, Kruskal-Wallis test) are used because the distribution for each component is not normally distributed based on Kolmogorov-Smirnov test, since the P-value(sig.) is smaller then the level of significance $\alpha = 0.05$. See table (5.1).

Table (5.1): 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

5.4.2 Validity of referees

The initial questionnaire has been given to a group of referees to judge its validity according to its content, the clearness of its items meaning, appropriateness to avoid any misunderstanding and to assure its linkage with the study objectives and hypothesis.

Based on the feedback, the questionnaire was modified distributed for a pilot study to test its statistical validity.

5.4.3 Validity of the questionnaire

Validity refers to the degree to which an instrument measures what it is supposed to be measuring (Pilot and Hungler, 1985). Validity has a number of different aspects and assessment approaches. Statistical validity is used to evaluate instrument validity, which include criterion-related validity and construct validity.

To insure the validity of the questionnaire, two statistical tests should be applied. The first test is Criterion-related validity test (Spearman test) which measures the correlation coefficient between each paragraph in one field and the whole field. The second test is structure validity test (Spearman test) that used to test the validity of the questionnaire structure by testing the validity of each field and the validity of the whole questionnaire. It measures the correlation coefficient between one filed and all the fields of the questionnaire that have the same level of similar scale.

5.4.3.1. Criterion Related Validity

Internal consistency of the questionnaire is measured by a scouting sample, which consisted of 30 questionnaires through measuring the correlation coefficients between each paragraph in one field and the whole filed.

Table (5.2) Correlation coefficient of each paragraph of Project Initiation and the total of this field

No.	Paragraph	Spearman Correlation Coefficient	P-Value (Sig.)
1.	Your plan contains project management techniques such as task management, resource allocation and budgeting.	0.894	0.000*
2.	Plan is supported from top management.	0.738	0.000*
3.	Employees are involved in setting the plan.	0.917	0.000*
4.	Experience Project manager Leads the team.	0.826	0.000*
5.	Plan Objectives are clear.	0.651	0.000*
6.	Plan requirement are well defined.	0.675	0.000*
7.	Plan scope and schedule are clear.	0.817	0.000*

* Correlation is significant at the 0.05 level

Table (5.2) clarifies the correlation coefficient for each paragraph of the Project Initiation and the total of the field. The p-values (Sig.) are less than 0.05, so the correlation coefficients of this field are significant at $\alpha = 0.05$, so it can be said that the paragraphs of this field are consistent and valid to be measure what it was set for.

Table (5.3) Correlation coefficient of each paragraph of Risk Assessment and the total of this field

No.	Paragraph	Spearman Correlation Coefficient	P-Value (Sig.)
1.	Risk assessment phase of business continuity and disaster recovery provides management with the necessary information to further evaluate or analyze each identified threat.	0.967	0.000*
2.	Risk assessment phase of business continuity and disaster recovery considers all possible threats to the information system, such as natural disaster, hardware and software failure, and human error.	0.885	0.000*
3.	Risk assessment phase of business continuity and disaster recovery identifies specific threats to business operations and measures each one's probability of occurrence.	0.941	0.000*
4.	Risk assessment phase of business continuity and disaster recovery discovers a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised.	0.989	0.000*
5.	In risk assessment, information is collected about, Hardware, Software, System interfaces, Data and information, and System and data criticality.	0.971	0.000*

* Correlation is significant at the 0.05 level

Table **(5.3)** clarifies the correlation coefficient for each paragraph of the Risk Assessment and the total of the field. The p-values (Sig.) are less than 0.05, so the correlation coefficients of this field are significant at $\alpha = 0.05$, so it can be said that the paragraphs of this field are consistent and valid to be measure what it was set for.

Table (5.4) Correlation coefficient of each paragraph of Business Impact Analysis and the total of this field

No.	Paragraph	Spearman Correlation Coefficient	P-Value (Sig.)
1.	During business impact analysis phase, critical business processes are identified and then analyzed.	0.852	0.000*
2.	Business impact analysis helps the organization to understand the degree of potential loss which could occur.	0.895	0.000*
3.	Your plan has a category system with all rating systems, the categories are clearly defined, and that there is a shared understanding of the proper use and scope of each.	0.905	0.000*
4.	Business impact analysis Informs a management decision on Maximum Tolerable Outage for each function, Maximum Tolerable Downtime, Recovery Time Objective .	0.932	0.000*

* Correlation is significant at the 0.05 level

Table **(5.4)** clarifies the correlation coefficient for each paragraph of the Business Impact Analysis and the total of the field. The p-values (Sig.) are less than 0.05, so the correlation coefficients of this field are significant at $\alpha = 0.05$, so it can be said that the paragraphs of this field are consistent and valid to be measure what it was set for.

Table (5.5) Correlation coefficient of each paragraph of Mitigation Strategy Development and the total of this field

No.	Paragraph	Spearman Correlation Coefficient	P-Value (Sig.)
1.	Your mitigation strategy contains development of strategies to accept, avoids, reduce, or transfer risks related to potential business disruptions.	0.677	0.000*
2.	Your mitigation strategy covers critical data and Records, to ensure that all critical information, activities, systems, and material is properly backed up and stored off-site	0.825	0.000*
3.	Your mitigation strategy covers Critical Systems and Infrastructure, to evaluate hardware and software solutions, vendors, and costs.	0.408	0.014*
4.	Your mitigation strategy covers information technology Recovery Systems, to grantee that all mission-critical information and equipment are appropriately safeguarded from any possible loss or damage.	0.550	0.001*
5.	Your mitigation strategy covers information technology backup Systems such, Disk SystemsDisk systems solutions continue to evolve in terms of capabilities	0.468	0.005*
6.	Your mitigation strategy covers anthers solutions such as: Remote Journaling: Remote journaling refers to the parallel processing of transactions to an alternate site.And Replication: Disk replication involves copying data on to a primary and secondary server.	0.569	0.001*

No.	Paragraph	Spearman Correlation Coefficient	P-Value (Sig.)
7.	Your mitigation strategy takes in account Standby Operating Systems.	0.728	0.000*
8.	Your mitigation strategy takes in account Desktop Solutions and user data.	0.535	0.001*
9.	Your mitigation strategy takes in account backing up and storing Software and Licensing at an offsite storage location.	0.547	0.001*
10.	Your mitigation strategy takes in account backing up and storing Web Sites through Load balancing strategies to ensure Web sites have high availability. Document Web Site. Web Site Programming. Web Site Coding.	0.601	0.000*

* Correlation is significant at the 0.05 level

Table **(5.5)** clarifies the correlation coefficient for each paragraph of the Mitigation Strategy Development and the total of the field. The p-values (Sig.) are less than 0.05, so the correlation coefficients of this field are significant at $\alpha = 0.05$, so it can be said that the paragraphs of this field are consistent and valid to be measure what it was set for.

Table (5.6) Correlation coefficient of each paragraph of Business Continuity/Disaster Recovery Plan Development and the total of this field

No.	Paragraph	Spearman Correlation Coefficient	P-Value (Sig.)
1.	In plan development you take mitigation strategies and identify methods for implementing those strategies, people, resources, and tasks needed to complete these activities	0.947	0.000*
2.	In plan development you state 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	0.998	0.000*
3.	In plan development you define communications plan to control the communication while a disaster occurred.	0.999	0.000*
4.	In plan development you define the initial actions taken once a system disruption or emergency has been detected.	0.991	0.000*

* Correlation is significant at the 0.05 level

Table **(5.6)** clarifies the correlation coefficient for each paragraph of the Business Continuity/Disaster Recovery Plan Development and the total of the field. The p-values (Sig.) are less than 0.05, so the correlation coefficients of this field are significant at $\alpha = 0.05$, so it can be said that the paragraphs of this field are consistent and valid to be measure what it was set for.

Table (5.7) Correlation coefficient of each paragraph of Business Continuity/Disaster Recovery Plan Testing and the total of this field

No.	Paragraph	Spearman Correlation Coefficient	P-Value (Sig.)
1.	Plan is tested on a periodic and regular basis.	0.924	0.000*
2.	The business continuity and disaster recovery plan should be exercised at least annually.	0.992	0.000*
3.	Plan testing determines whether the right resources have been identified	0.962	0.000*
4.	Plan testing identifies gaps or weaknesses in the plan.	0.990	0.000*

* Correlation is significant at the 0.05 level

Table **(5.7)** clarifies the correlation coefficient for each paragraph of the Business Continuity/Disaster Recovery Plan Testing and the total of the field. The p-values (Sig.) are less than 0.05, so the correlation coefficients of this field are significant at $\alpha = 0.05$, so it can be said that the paragraphs of this field are consistent and valid to be measure what it was set for.

Table (5.8) Correlation coefficient of each paragraph of Business Continuity/Disaster Recovery Plan Auditing and the total of this field

No.	Paragraph	Spearman Correlation Coefficient	P-Value (Sig.)
1.	Plan auditing is done to ensure information technology risk mitigation strategies are in place and properly implemented/configured.	0.994	0.000*
2.	Plan auditing is done to ensure systems identified by the business continuity and disaster recovery plan are still in place and functioning.	0.996	0.000*
3.	By auditing data reviewed regarding various systems to ensure they are still compliant with the business continuity and disaster recovery plans.	0.934	0.000*

* Correlation is significant at the 0.05 level

Table **(5.8)** clarifies the correlation coefficient for each paragraph of the Business Continuity/Disaster Recovery Plan Auditing and the total of the field. The p-values (Sig.) are less than 0.05, so the correlation coefficients of this field are significant at $\alpha = 0.05$, so it can be said that the paragraphs of this field are consistent and valid to be measure what it was set for.

Table (5.9) Correlation coefficient of each paragraph of Business Continuity/Disaster Recovery Plan Maintenance and the total of this field

No.	Paragraph	Spearman Correlation Coefficient	P-Value (Sig.)
1.	The plan use a revision numbering system, so team members know whether they have the latest version of the plan.	0.947	0.000*
2.	Key contact information are revised, reviewed, and updated regularly.	0.994	0.000*
3.	There are up-to-date copies of the business continuity and disaster recovery plan off-site in the event the building is inaccessible.	0.982	0.000*
4.	Plan maintenance procedures are Documented, to avoid introducing additional risk into the project.	0.994	0.000*

* Correlation is significant at the 0.05 level

Table **(5.9)** clarifies the correlation coefficient for each paragraph of the Business Continuity/Disaster Recovery Plan Maintenance and the total of the field. The p-values (Sig.) are less than 0.05, so the correlation coefficients of this field are significant at $\alpha = 0.05$, so it can be said that the paragraphs of this field are consistent and valid to be measure what it was set for.

Table (5.10) Correlation coefficient of each paragraph of Business Continuity/Disaster Recovery Training and the total of this field

No.	Paragraph	Spearman Correlation Coefficient	P-Value (Sig.)
1.	Staff is well trained on the plan activation and treatment.	0.944	0.000*
2.	Company performs training needs assessment to fill the gaps in skills.	0.942	0.000*
3.	Plan Training identified the training Scope, Objectives, Timelines, and Requirements.	0.993	0.000*
4.	Company finds various training programs online that people can attend on their own schedule.	0.991	0.000*
5.	Training Monitoring is done to ensure key personnel have actually attended required training.	0.976	0.000*

* Correlation is significant at the 0.05 level

Table **(5.10)** clarifies the correlation coefficient for each paragraph of the Business Continuity/Disaster Recovery Training and the total of the field. The p-values (Sig.) are less than 0.05, so the correlation coefficients of this field are significant at $\alpha = 0.05$, so it can be said that the paragraphs of this field are consistent and valid to be measure what it was set for.

5.4.3.2. Structure Validity of the Questionnaire

Structure validity is the second statistical test that used to test the validity of the questionnaire structure by testing the validity of each field and the validity of the whole questionnaire. It measures the correlation coefficient between one filed and all the fields of the questionnaire that have the same level of liker scale.

The researcher assessed the fields' structure validity by calculating the correlation coefficients of each field of the questionnaire and the whole of questionnaire.

Table (5.11) Correlation coefficient of each field and the whole of questionnaire

No.	Field	Spearman Correlation Coefficient	P-Value (Sig.)
1.	Project Initiation	0.853	0.000*
2.	Risk Assessment	0.867	0.000*
3.	Business Impact Analysis	0.790	0.000*
4.	Mitigation Strategy Development	0.576	0.001*
5.	Business Continuity/Disaster Recovery Plan Development	0.745	0.000*
6.	Business Continuity/Disaster Recovery Plan Testing	0.458	0.006*
7.	Business Continuity/Disaster Recovery Plan Auditing	0.900	0.000*
8.	Business Continuity/Disaster Recovery Plan Maintenance	0.877	0.000*
9.	Business Continuity/Disaster Recovery Plan Testing, Auditing, and Maintenance	0.883	0.000*
10.	Business Continuity/Disaster Recovery Training	0.712	0.000*

* Correlation is significant at the 0.05 level

Table (5.11) clarifies the correlation coefficient for each filed and the whole questionnaire. The p-values (Sig.) are less than 0.05, so the correlation coefficients of all the fields are significant at $\alpha = 0.05$, so it can be said that the fields are valid to be measured what it was set for to achieve the main aim of the study.

5.5. Reliability of the Questionnaire

The reliability of an instrument is the degree of consistency which measures the attribute; it is supposed to be measuring (Polit & Hunger,1985). The less variation an instrument produces in repeated measurements of an attribute, the higher its reliability. Reliability can be equated with the stability, consistency, or dependability of a measuring tool. The test is repeated to the same sample of people on two occasions and then compares

the scores obtained by computing a reliability coefficient (Polit & Hunger, 1985).

5.5.1 Cronbach's Coefficient Alpha

This method is used to measure the reliability of the questionnaire between each field and the mean of the whole fields of the questionnaire. The normal range of Cronbach's coefficient alpha value between 0.0 and + 1.0, and the higher values reflects a higher degree of internal consistency. The Cronbach's coefficient alpha was calculated for each field of the questionnaire.

Table (5.12) Cronbach's Alpha for each filed of the questionnaire and the entire questionnaire.

No.	Field	Cronbach's Alpha	Reliability *
1.	Project Initiation	0.978	0.989
2.	Risk Assessment	0.991	0.996
3.	Business Impact Analysis	0.958	0.979
4.	Mitigation Strategy Development	0.873	0.934
5.	Business Continuity/Disaster Recovery Plan Development	0.988	0.994
6.	Business Continuity/Disaster Recovery Plan Testing	0.987	0.993
7.	Business Continuity/Disaster Recovery Plan Auditing	0.988	0.994
8.	Business Continuity/Disaster Recovery Plan Maintenance	0.987	0.993
9.	Business Continuity/Disaster Recovery Plan Testing, Auditing, and Maintenance	0.967	0.983
10.	Business Continuity/Disaster Recovery Training	0.996	0.998
	Total	0.981	0.991

* Reliability = Square root of Cronbach's Alpha

Table (5.12) shows the values of Cronbach's Alpha for each filed of the questionnaire and the entire questionnaire. For the fields, values of Cronbach's Alpha were in the range from 0.873 and 0.934. Therefore, the reliability scores range from 0.934 and 0.998. This range is considered high; the result ensures the reliability of each field of the questionnaire. Cronbach's Alpha equals 0.981 for the entire questionnaire and the corresponding reliability score is 0.991 which indicates an excellent reliability of the entire questionnaire.

Thereby, it can be said that the researcher proved that the questionnaire was valid, reliable, and ready for distribution for the population sample.

5.6. Sample Characteristics

Personal Characteristics:

1. Qualification :

Table (5.13) **Sample Qualification**

Qualification	Frequency	Percent
Diploma	4	6.5
Bachelor	49	79.03
Master	8	12.9
Doctorate	1	1.6
Total	62	100.0

This reflects the proper background education that the information technology managers of the Palestinian companies have.

2. Job Title:

Table (5.14) **Sample Job Titles**

Job Title	Frequency	Percent
Manager	25	40.3
Supervisor	28	45.2
Engineer/programmer/Developer	9	14.5
Total	62	100.0

It could be noticed from table 5.14 that the majority of respondents (85.5%) are in managerial/Supervisory or administrative posts, while the others are in different technical posts (Engineer/programmer/Developer).

This indicates that majority of research respondents were working as decision makers in their departments, which reflects their level of effectiveness in their jobs.

3. Specialization:

Table (5.15) **Sample Specializations**

Specialization	Frequency	Percent
Computer Engineer	24	38.7
Computer science	24	38.7
Business Administration	10	16.1
others	4	6.5
Total	62	100.0

This indicates that 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.

4. Experience:

Table (5.16) **Sample Experiences**

Experience	Frequency	Percent
Less than 5 years	8	12.9
5-10 years	12	19.4
11-15 years	20	32.3
More than 15years	22	35.5
Total	62	100.0

It is clear from Table (5.16) that most (67.8%) of the respondents are having not less than ten years of experience, while others (29.3%) having not less than two years of experience, this mean that the respondents having a reasonable experience in their working field. 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.

5. Age:

Table (5.17) Sample **Ages**

Age	Frequency	Percent
Less than 25	2	3.2
25- Less than 35	34	54.8
35 - Less than 45	22	35.5
45 and older	4	6.5
Total	62	100.0

This properly reflects how much power they have to lead companies due to their profession.

b) Company Profile:

1. Number of workers in the company:

Table (5.18) **Number of workers in the company**

Number of workers in the company	Frequency	Percent
Less than 10	4	6.5
10-50	8	12.9
51-100	14	22.6
More than 100	36	58.1
Total	62	100.0

This reflects that most Palestinian companies consider as large companies, so it has to apply business continuity and disaster recovery planning in their businesses.

2. Company Type:

Table (5.19) **Company Types**

Company Type	Frequency	Percent
Industrial	22	35.5
Trading	4	6.5
Service	34	54.8
Others	2	3.2
Total	62	100.0

This reflects their diversity.

3. Information Technology Services done by:

Table (5.20) **Information technology Services**

Information technology Services	Frequency	Percent
Internal Department	30	48.4
Outsourcing	12	19.4
Mixed	20	32.3
Total	62	100.0

This reflects the diversity in introduced information technology services in Palestinian companies.

4. Information Technology Department Sections:

Table (5.21) **Information Technology Department Sections**

Information technology Department Sections	Frequency	Percent
One	42	67.7
Two	6	9.7
Three	10	16.1
More than 3	4	6.5
Total	62	100.0

It is clear from Table (5.21) that (67.7%) of respondents' companies had one section in information technology department, (9.7%) had two sections, (16.1%) had three sections, and (16.1%) had more than 3 sections. This reflects the dependence on information technology services in targeted companies, but actually reflects also the less of spatiality inside information technology departments.

5. Number of employees in information technology department

Table (5.22) **Information Technology Department Employees**

Number of employees	Frequency	Percent
Less than 3	36	58.1
3-5	10	16.1
6-10	10	16.1
More than 10	6	9.7
Total	62	100.0

This reflects the diversity in the size and type of information technology services

introduced to companies, but 58.1% less than 3 workers actually indicates weaknesses in the human resource requirements in information technology department in the targeted companies.

Part 2:

5.7. Company Disasters Analysis.

Has your company ever faced a disaster threat?

Table (5.23) Companies faced threats

Faced a disaster threats	Frequency	Percent
Yes	34	54.8
No	28	45.2
Total	62	100.0

This reflects the importance of planning for business continuity and disaster recovery planning.

IF yes, what is the disaster type?

Table (5.24) **Disaster types**

Disaster type	N	Percent
Human Caused	6	16.7%
Infrastructure Threat	30	83.3%

This reflects that most of disasters were made suddenly, such as breakdown in hardware, or electricity interruptions effects.

Disaster strikes

Table (5.25) **Disaster effects**

Disaster strikes	N	Percent
Hardware	18	39.1%
Software	26	56.5%
Staff	2	4.3%

This reflects the importance of existing comprehensive plans where there was diversity in the targeted resources. Hardware disaster such as servers' breakdown or network interruption, but software disasters such as data deletion.

Chapter Six:

Empirical Framework Hypothesis Testing & Discussion

Preface:

In this chapter, data analysis results will be explained, analyzed and discussed to measure the level of existence of Business continuity and disaster recovery planning in information technology departments of the listed companies. This chapter will discuss the following main issues:

1. Type of data

2. Analyzing and testing the dimensions of the questionnaire

6.1. Type of data

In small sample studies usually conducting Kolomogrov Simrnov 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 then the level of significance $\alpha = 0.05$ .So data is non-parametric. See table (6.1).

Table (6.1): 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

6.2. 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 that the level of significance, $\alpha = 0.05$, then the mean is significantly different from a hypothesized value 6. The sign of

the Test value indicates whether the mean is significantly greater or smaller than hypothesized value 6. On the other hand, if the P-value (Sig.) is greater than the level of significance, $\alpha = 0.05$, then the mean is insignificantly different from a hypothesized value 6.

6.2.1. The first hypothesis:

"There is a significant difference in the level of existence of the seven component of Business Continuity and Disaster Recovery between the responded companies (Project initiation techniques, Risk Assessment, Business impact analysis, Mitigation strategy, Plan development, Testing, auditing and maintaining, Training)."

1- Project Initiation

Table (6.2) revealed that all the mean values of paragraphs related to project initiation dimension were more than 6 and P-value less than .05, which means that most project initiation techniques were found in the business continuity and disaster recovery planning in information technology departments of the targeted companies, for example plans of targeted companies identified the business resources, and budgets (77.4%). Also there was a support to the plans from the top management (75.34%). This is in addition to the clearly identified objectives (76.38%) and requirements (76.38%). Moreover the targeted companies appointed experience managers to lead the plans (76.9%), and all of the related employees participated in the setting up the plan (72.59%).

Overall the total score of the dimension "project initiation" was (76.3%) and P-value was (0%). 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 (as explained in the analysis) 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.

The results of this dimension agree with some previous studies as follows:

1. (Kon, 1997): The study reported that business continuity planning has to compromise top management approval and support.
2. (Ernest, 1999): This study reported that managers in information technology area are responsible for contingency planning for the whole business.
3. (Wong and others, 1994):This paper reported a set of procedures to develop a successful disaster recovery plans which included top management support, adequate financial support, to understand the objectives of the plan, and to define the scope of the plan.
4. (Chow, 2000): This paper reported the top five critical success factors of disaster recovery plan, which included top management support, and adequate financial support.
5. (Moh, 1996): This paper suggested a methodology to develop suitable business continuity and disaster recovery plan, which included project planning.
6. (Carlson and Parker, 1998): This study urged that without the support of management disaster recovery plan will not be successfully.

Table (6.2): The mean and test value for "Project Initiation"

No	Paragraph	Mean	Proportional Mean%	Test value	P-value (Sig.)	Rank
1.	Your plan contains project management techniques such as task management, resource allocation and budgeting.	7.74	77.42	4.68	0.000*	1
2.	Plan is supported from top management.	7.53	75.34	3.92	0.000*	5
3.	Employees are involved in setting the plan.	7.26	72.59	3.78	0.000*	7
4.	Experience Project manager Leads the team.	7.69	76.90	3.95	0.000*	2
5.	Plan Objectives are clear.	7.59	75.86	4.12	0.000*	4
6.	Plan requirement are well defined.	7.64	76.38	4.12	0.000*	3
7.	Plan scope and schedule are clear.	7.29	72.93	2.80	0.003*	6
	Project Initiation	7.63	76.31	4.78	0.000*	

* The mean is significantly different from 6

2- Risk Assessment

Table (6.3) revealed that all the mean values of paragraphs related to Risk Assessment dimension more than 6 and P-value less than .05, which means that most Risk Assessment procedures were followed in the business continuity and disaster recovery planning in information technology departments of the targeted companies, for example risk assessment of targeted companies gave the management the required information to complete the analysis of the identified threats (76.55%), all of potential threats are considered (76.21%), all required information is collected (76.21%), possibility of each threat is measured(76.03%), and it discovered the weaknesses in the security procedures of the applied system(74.31%).

At overall the total score of the dimension " Risk Assessment " was (75.86%) and P-value was (0%).It means that the majority of the companies are practicing good, and semi-deep, and valuable risk assessment procedures, so that results can help in identifying and treating the expected threats.

This is due to the serious steps followed in assessment, in order to avoid the consequences of weak 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.

The results obtained, come on line with other previous studies as follows:

1. (Taye, 2008): This study revealed that (61%)of Palestinian companies identified the events that could cause interruptions the business.
2. (Sharon , 1998): This paper reported six major priorities to create disaster recovery plan which included conducting risk analysis.
3. (Wong and others, 1994): This paper suggested steps to develop successful disaster recovery plans, which included performing risk assessment.

Table (6.3): The mean and test value for "Risk Assessment"

No	Paragraph	Mean	Proportional Mean%	Test value	P-value(Sig.)	Rank
1.	Risk assessment phase of business continuity and disaster recovery provides management with the necessary information to further evaluate or analyze each identified threat.	7.66	76.55	4.67	0.000*	1
2.	Risk assessment phase of business continuity and disaster recovery considers all possible threats to the information system, such as natural disaster, hardware and software failure, and human error.	7.62	76.21	4.30	0.000*	2
3.	Risk assessment phase of business continuity and disaster recovery identifies specific threats to business operations and measures each one's probability of occurrence.	7.60	76.03	4.67	0.000*	4
4.	Risk assessment phase of business continuity and disaster recovery discovers a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised.	7.43	74.31	3.90	0.000*	5
5.	In risk assessment, information is collected about, Hardware, Software, System interfaces, Data and information, and System and data criticality.	7.62	76.21	4.30	0.000*	2
	Risk Assessment	7.59	75.86	4.58	0.000*	

* The mean is significantly different from 6

3- Business Impact Analysis

Table (6.4) revealed that all the mean values of paragraphs related to Business Impact Analysis dimension more than 6 and P-value less than .05, which means that most Business Impact Analysis procedures were found in the business continuity and disaster recovery planning in information technology departments of the targeted companies, for example Business Impact Analysis of targeted companies identified and analyzed critical business process(78.97%), gave the companies a comprehensive information about the potential loss (76.38%), it had categories with rating of the impacts (71.72%), and Maximum Tolerable Outage for each function, Maximum Tolerable Downtime, Recovery Time Objective are given by Business Impact Analysis(69.31%).

At overall the total score of the dimension "Business Impact Analysis" was (74.05%) and P-value was (0%).It means that the majority of the targeted companies 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 companies.

The results of this dimension come on line with other previous researchers:

1. (Kon,1997): The study reported that business continuity planning has to compromise performing business impact analysis.
2. (Pat, 1995): This study revealed that (59%) of the companies performed Business impact analysis, but they have unstructured approach to conducting business impacts analysis.
3. (Lumpur, 2007): This study revealed that almost of 70% of companies had undertaken business impact analysis.
4. (Moh, 1996): This paper suggested a methodology to develop suitable business continuity plan which included business impact analysis.
5. (Wong and others, 1994): This paper suggested steps to develop successful disaster recovery plans, which included performing business impact analysis.
6. (Bandyopadhya, 2002): This study indicated that (53.72%) of companies business impacts analysis.

Table (6.4): The mean and test value for "Business Impact Analysis"

No	Paragraph	Mean	Proportional Mean%	Test value	P-value(Sig.)	Rank
1.	During business impact analysis phase, critical business processes are identified and then analyzed.	7.90	78.97	4.94	0.000*	1
2.	Business impact analysis helps the organization to understand the degree of potential loss which could occur.	7.64	76.38	4.40	0.000*	2
3.	Your plan has a category system with all rating systems, the categories are clearly defined, and that there is a shared understanding of the proper use and scope of each.	7.17	71.72	3.21	0.001*	3
4.	Business impact analysis Informs a management decision on Maximum Tolerable Outage for each function, Maximum Tolerable Downtime, Recovery Time Objective.	6.91	69.14	3.03	0.001*	4
	Business Impact Analysis	7.41	74.05	4.22	0.000*	

* The mean is significantly different from 6

4- Mitigation Strategy Development

Table (6.5) revealed that all the mean values of paragraphs related to Mitigation Strategy Development dimension more than 6 and P-value less than .05, which means that most Mitigation Strategy actions were well applied in the business continuity and disaster recovery planning in information technology departments of the targeted companies, for example Mitigation Strategies of targeted companies had proper internal backup strategies (91.72%), it covered critical data and records (90.22%), desktops and users were well treated in the strategies (89.66%).

At overall the total score of the dimension "Mitigation Strategy Development" was

(82.81%) and P-value was (0%).It means that the majority of the targeted companies 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 companies had good skills and experience in such field. Moreover most of companies can provide the required materials and equipments to the team, because of the low cost relatively with cost of consequences in case of disaster attract consequences.

The findings of this dimension are shared with other previous studies:

1. (Taye, 2008): About (63.4%) of Palestinian information technology companies developed plans to restore business operations within the required timeframe.
2. (Kon, 1997): The study reported that business continuity planning has to compromise determining the strategies of business continuity associated recovery process.
3. (Lumper,2007): The study reported that most of companies preferred both in-site and off-site disaster recovery environments, 92% of respondents have a recovery time and point objective of 0 hours to 24 hours, Large multinational companies tend to have less than three hours of recovery time and point objective.
4. (Jackson, 2006): This paper highlighted the necessary solutions that businesses should implement to ensure continuity including: server backups, web mail, remote/home working, server based computing.
5. (Pat, 1995): This study reported that the following issues have to be founded in business continuity plan: Hot site-cold/site--warm site requirements, vital records recovery, Telecommunications recovery, Electronics recovery/restoration.
6. (Moh, 1996): This paper suggested a methodology to develop suitable business continuity plan which included recovery strategy.
7. (Chow, 2000): This paper showed that both of in-site and off-site backup were considered as significance.

Table (6.5): The mean and test value for "Mitigation Strategy Development"

No	Paragraph	Mean	Proportional Mean%	Test value	P-value(Sig.)	Rank
1.	Your mitigation strategy contains development of strategies to accept, avoids, reduce, or transfer risks related to potential business disruptions.	8.36	83.62	5.77	0.000*	6
2.	Your mitigation strategy covers critical data and Records, to ensure that all critical information, activities, systems, and material is properly backed up and stored off-site.	9.02	90.22	6.96	0.000*	2
3.	Your mitigation strategy covers Critical Systems and Infrastructure, to evaluate hardware and software solutions, vendors, and costs.	8.76	87.59	6.28	0.000*	4
4.	Your mitigation strategy covers information technology Recovery Systems, to grantee that all mission-critical information and equipment are appropriately safeguarded from any possible loss or damage.	8.45	84.48	5.75	0.000*	5
5.	Your mitigation strategy covers information technology backup Systems such, Disk systems solutions such: RAID, And Data backup strategy, Full backup, Incremental method Differential method.	9.17	91.72	6.96	0.000*	1
6.	Your mitigation strategy covers anthers solutions such as: Remote Journaling: Remote journaling refers to the parallel processing of transactions to an alternate site. And Replication: Disk replication involves copying data on to a primary and secondary server.	6.82	68.21	1.68	0.046*	9
7.	Your mitigation strategy takes in account Standby Operating Systems.	8.34	83.45	5.38	0.000*	7

No	Paragraph	Mean	Proportional Mean%	Test value	P-value(Sig.)	Rank
8.	Your mitigation strategy takes in account Desktop Solutions and user data.	8.97	89.66	6.82	0.000*	3
9.	Your mitigation strategy takes in account backing up and storing Software and Licensing at an offsite storage location.	8.31	83.10	5.39	0.000*	8
10	Your mitigation strategy takes in account backing up and storing Web Sites through Load balancing strategies to ensure Web sites have high availability. Document Web Site. Web Site Programming. Web Site Coding.	6.53	65.34	0.95	0.170	10
	Mitigation Strategy Development	8.28	82.81	6.43	0.000*	

* The mean is significantly different from 6

5- Business Continuity/Disaster Recovery Plan Development

Table (6.6) 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 companies, for example Plan Development of targeted companies 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 companies 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 companies' 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 companies. While the P-Value more than 5%, it reflected that the targeted companies did not agree to a unified and similar answer in developing their plan. This was due to the fact that not all of companies had written their plan and not all of the companies had such plans, which reflect a weakness in writing the plans in some of companies.

The results of this dimension come on line with other previous researchers:

1. (Pitt and Goyal, 2004): The result of this study demonstrated that (50%) of respondents have fully integrated or comprehensive business continuity plans.
2. (Wong and others, 1994): This paper suggested steps to develop successful disaster recovery plans, which included develop and implement the plan.
3. (Moh, 1996): This paper suggested a methodology to develop suitable business continuity and disaster recovery plan, which included Plan development.

Table (6.6): The mean and test value for "Business Continuity/Disaster Recovery Plan Development"

No	Paragraph	Mean	Proportional Mean%	Test value	P-value(Sig.)	Rank
1.	In plan development you take mitigation strategies and identify methods for implementing those strategies, people, resources, and tasks needed to complete these activities.	6.88	68.79	2.24	0.013*	1

No	Paragraph	Mean	Proportional Mean%	Test value	P-value(Sig.)	Rank
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	1.40	0.081	

* The mean is significantly different from 6

6A- Business Continuity/Disaster Recovery Plan Testing

Table (6.7) 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 companies, for example Plan Testing of targeted companies 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 companies 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

companies' 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 (6.7): The mean and test value for "Business Continuity/Disaster Recovery Plan Testing"

No	Paragraph	Mean	Proportional Mean%	Test value	P-value(Sig.)	Rank
1.	Plan is tested on a periodic and regular basis.	8.07	80.69	5.22	0.000*	
2.	The business continuity and disaster recovery plan should be exercised at least annually.	8.02	80.17	4.67	0.000*	
3.	Plan testing determines whether the right resources have been identified	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 Testing	8.08	80.78	5.12	0.000*	

* The mean is significantly different from 6

6B- Business Continuity/Disaster Recovery Plan Auditing

Table (6.8) revealed that all the mean values of paragraphs related to Business Continuity/Disaster Recovery Plan Auditing dimension more than 6 and P-value less than .05, which means that most Plan Auditing procedures were well applied in the business continuity and disaster recovery planning in information technology departments of the

targeted companies, for example auditing ensured that systems were still compliant with the plan (73.45%), system were in their places (71.55%), and the mitigations strategies are valid (71.03%).

At overall the total score of the dimension "Business Continuity/Disaster Recovery Plan Auditing" was (72.01%) and P-value was (0.01). It means that the majority of the targeted companies had accurate, rich, and comprehensive procedures in auditing their plans.

It was concluded that 72.01% of the business continuity and disaster recovery plans auditing procedures applied in the targeted companies ensured that auditing procedures were good and enough to keep the plan ready to face any potential disaster.

Table (6.8): The mean and test value for "Business Continuity/Disaster Recovery Plan Auditing"

No	Paragraph	Mean	Proportional Mean%	Test value	P-value(Sig.)	Rank
1.	Plan auditing is done to ensure information technology risk mitigation strategies are in place and properly implemented/configured.	7.10	71.03	2.80	0.003*	3
2.	Plan auditing is done to ensure systems identified by the business continuity and disaster recovery plan are still in place and functioning.	7.16	71.55	2.80	0.003*	2
3.	By auditing data reviewed regarding various systems to ensure they are still compliant with the business continuity and disaster recovery plans.	7.34	73.45	3.24	0.001*	1
	Business Continuity/Disaster Recovery Plan Auditing	7.20	72.01	3.24	0.001*	

- The mean is significantly different from 6

6C: Business Continuity/Disaster Recovery Plan Maintenance

Table (6.9) revealed that most the mean values of paragraphs related to Business Continuity/Disaster Recovery Plan Maintenance dimension more than 6 and P-value less than .05, which means that most Plan Maintenance procedures were well applied in the business continuity and disaster recovery planning in information technology departments of the targeted companies, for example plans maintenance procedures applied in the targeted companies ensured to make off-site copy of the last updated version of the plan(68.01%), it ensured to use a revision numbering system to guarantee the usages of the last updated copy of the plan, and to avoid the ambiguity(68.10%), and maintained actions were documented to avoid any misunderstanding, bad interpretations, or Forgotten(71.03%).

At overall the total score of the dimension "Business Continuity/Disaster Recovery Plan Maintenance" was (71.22%) and P-value was (0.001). It means that the majority of the targeted companies had accurate, rich, and comprehensive procedures in maintenance their plans.

It was concluded that 71.22% of the business continuity and disaster recovery plans maintenance procedures applied in the targeted companies were accurate, and 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.

Table (6.9): The mean and test value for "Business Continuity/Disaster Recovery Plan Maintenance"

No	Paragraph	Mean	Proportional Mean%	Test value	P-value(Sig.)	Rank
1.	The plan use a revision numbering system, so team members know whether they have the latest version of the plan.	7.40	74.02	3.40	0.000*	1

No	Paragraph	Mean	Proportional Mean%	Test value	P-value(Sig.)	Rank
2.	Key contact information are revised, reviewed, and updated regularly.	7.17	71.72	3.19	0.001*	2
3.	There are up-to-date copies of the business continuity and disaster recovery plan off-site in the event the building is inaccessible.	6.81	68.10	1.43	0.077	4
4.	Plan maintenance procedures are Documented, to avoid introducing additional risk into the project.	7.10	71.03	2.97	0.001*	3
	Business Continuity/Disaster Recovery Plan Maintenance	7.12	71.22	3.24	0.001*	

* The mean is significantly different from 6

6- Business Continuity/Disaster Recovery Plan Testing, Auditing, and Maintenance.

At overall the total score of the dimension "Business Continuity/Disaster Recovery Plan Testing, Auditing, and Maintenance" equals 7.49 (74.91%), test value=4.07, and P-value =0.000 which is smaller than the level of significance $\alpha = 0.05$. Then the mean of this component is significantly greater than the hypothesized value 6.

It was concluded that plan testing, auditing, and maintaining procedures applied in the targeted companies 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.

The results of this dimension come on line with other previous researchers:

1. (Taye, 2008): About (65.9%) of Palestinian information technology companies had a single framework of business continuity plan which was

maintained to ensure consistency and identifying priorities for testing, And about (56.1%) testing their plans regularly.

2. (Kon, 1997): The study reported that business continuity planning has to compromise testing, reviewing, and updating the plan.
3. (Lumper,2007): The study reported that the majority of the respondents had their business continuity plans tested less than a year ago, with 40% testing business continuity and disaster recovery plans tested in the last six months.
4. (Pitt and Goyal, 2004): The paper shows that the viability and effectiveness of Business continuity planning is dependent on regular review, audit and testing.
5. (Sharon , 1998): This paper reported six major priorities to create disaster recovery plan which included testing the plans.
6. (Moh, 1996): This paper suggested a methodology to develop suitable business continuity and disaster recovery plan, which included Plan testing.

Table (6.10): The mean and test value for "Business Continuity/Disaster Recovery Plan Testing, Auditing, and Maintenance"

Item	Mean	Proportional Mean%	Test value	P-value(Sig.)
Business Continuity/Disaster Recovery Plan Testing, Auditing, and Maintenance	7.49	74.91	4.07	0.000*

* The mean is significantly different from 6

7- Business Continuity/Disaster Recovery Training

Table (6.11) revealed that most the mean values of paragraphs related to Business Continuity/Disaster Recovery Plan Training dimension more than 6 and P-value less than .05, which means that Plan training were well practiced in information technology departments of the targeted companies, for example most training initiations' procedures were followed up by the targeted companies (82.22%), most training monitoring procedures were followed up by the targeted companies (81.00%),

At overall the total score of the dimension "Business Continuity/Disaster Recovery

Training" equals 8.15 (81.45%), test value=5.71, and P-value =0.000 which is smaller than the level of significance $\alpha = 0.05$. Then the mean of this component is significantly greater than the hypothesized value 6.

It was concluded that most companies 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.

Table (6.11): The mean and test value for "Business Continuity/Disaster Recovery Training"

No	Paragraph	Mean	Proportional Mean%	Test value	P-value(Sig.)	Rank
1.	Staff is well trained on the plan activation and treatment.	8.12	81.17	5.83	0.000*	3
2.	Company performs training needs assessment to fill the gaps in skills.	8.18	81.83	5.83	0.000*	2
3.	Plan Training identified the training Scope, Objectives, Timelines, and Requirements.	8.22	82.22	5.80	0.000*	1
4.	Company finds various training programs online that people can attend on their own schedule.	8.11	81.05	5.43	0.000*	4
5.	Training Monitoring is done to ensure key personnel have actually attended required training.	8.10	81.00	5.43	0.000*	5
	Business Continuity/Disaster Recovery Training	8.15	81.45	5.71	0.000*	

* The mean is significantly different from 6

Level of existence of business continuity and disaster recovery planning in the listed companies.

Table (6.12) revealed that the mean of the seven components together equals 7.69 (76.90%), and P-value =0.000 which is smaller than the level of significance $\alpha = 0.05$. Then the mean of all components together is significantly greater than the hypothesized value 6.

It was concluded that the most existed component in the plan was the mitigation strategies(80.28%). This is because most of companies 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 (67.28%). This is because not all of information technology leaders are organized, and they depend totally on their minds memory, or they were not strongly requested to write a plan to mitigate such cases.

Table (6.12): The mean and test value for "Seven components together and the overall of business continuity and disaster recovery plan"

Paragraph	Mean	Proportional Mean%	Test value	P-value(Sig.)	Rank
Project Initiation.	7.63	76.31	4.78	0.000*	4
Risk Assessment.	7.59	75.86	4.58	0.000*	5
Business Impact Analysis.	7.41	74.05	4.22	0.000*	7
Mitigation Strategy Development.	8.28	82.81	6.43	0.000*	1
Business Continuity/Disaster Recovery Plan Development.	6.73	67.28	1.40	0.081	10
Business Continuity/Disaster Recovery Plan Testing.	8.08	80.78	5.12	0.000*	3
Business Continuity/Disaster Recovery Plan Auditing .	7.20	72.01	3.24	0.001*	8
Business Continuity/Disaster Recovery Plan Maintenance.	7.12	71.22	3.24	0.001*	9
Business Continuity/Disaster Recovery Plan Testing, Auditing, and Maintenance.	7.49	74.91	4.07	0.000*	6
Business Continuity/Disaster Recovery Training.	8.15	81.45	5.71	0.000*	2
Seven components together	7.69	76.90	5.46	0.000*	

*The mean is significantly different from 6

6.2.2. The second hypothesis:

"There is a correlation between the level of existence of Business Continuity and Disaster Recovery and the seven components."

Table (6.13) Correlation coefficient of each field and the whole of questionnaire

No.	Field	Spearman Correlation Coefficient	P-Value (Sig.)
1.	Project Initiation	0.791	0.000*
2.	Risk Assessment	0.856	0.000*
3.	Business Impact Analysis	0.817	0.000*
4.	Mitigation Strategy Development	0.687	0.000*
5.	Business Continuity/Disaster Recovery Plan Development	0.777	0.000*
6.	Business Continuity/Disaster Recovery Plan Testing	0.450	0.000*
7.	Business Continuity/Disaster Recovery Plan Auditing	0.846	0.000*
8.	Business Continuity/Disaster Recovery Plan Maintenance	0.867	0.000*
9.	Business Continuity/Disaster Recovery Plan Testing, Auditing, and Maintenance	0.872	0.000*
10.	Business Continuity/Disaster Recovery Training	0.721	0.000*

* Correlation is significant at the 0.05 level

Table **(6.13)** clarifies the correlation coefficient between the level of existence of Business Continuity and Disaster Recovery and the seven components.

For Project Initiation, the spearman correlation coefficient equals 0.791 and the p-values (Sig.) equals 0.000 which is smaller than the level of significance $\alpha = 0.05$. Then there exist significant relationships between Project Initiation and the seven components.

This means that more existence of the project initiation techniques, the more existence of good and effective business continuity and disaster recovery plan.

For Risk Assessment, the spearman correlation coefficient equals 0.856 and the p-values (Sig.) equals 0.000 which means that there is significant relationship between Risk Assessment and the seven components.

This means that in order to increase the level of existence of good and effective BC/ disaster recovery plan, better accurate and deep risk assessment should be practiced by companies.

For Business Impact Analysis, the spearman correlation coefficient equals 0.817. Then there is a significant relationship between business impact analysis and the seven components.

This means that in order to increase the level of existence of good and effective BC/ disaster recovery plan, better accurate and deep business impact analysis should be practiced by companies.

For Mitigation Strategy Development, the spearman correlation coefficient equals 0.687, which means that there is a significant relationship between Mitigation Strategy Development and the seven components. This means that the more existence of mitigation strategies, the more existence of good and effective business continuity and disaster recovery plan.

For Business Continuity/Disaster Recovery Plan Development, the spearman correlation coefficient equals 0.777, which means that there is a significant relationship between Business Continuity/Disaster Recovery Plan Development and the seven components.

This means that in order to increase the level of existence of good and effective BC/ disaster recovery plan, better comprehensive Business Continuity/Disaster Recovery Plan Development should be formulated by companies.

For Business Continuity/Disaster Recovery Plan Testing, the spearman correlation coefficient equals 0.450 which means that there is a significant relationship between Business Continuity/Disaster Recovery Plan Testing and the seven components. This means that the more existence of accurate and deep plan testing, the more existence of good and effective business continuity and disaster recovery plan.

For Business Continuity/Disaster Recovery Plan Auditing, the spearman correlation coefficient equals 0.846 which means that there is a significant relationship between

Business Continuity/Disaster Recovery Plan Auditing and the seven components. This means that the more existence of accurate and deep plan auditing, the more existence of good and effective business continuity and disaster recovery plans.

For Business Continuity/Disaster Recovery Plan Maintenance, the spearman correlation coefficient equals 0.867 and which means that there is a significant relationship between Business Continuity/Disaster Recovery Plan Maintenance and the seven components. This means that the more existence of accurate and deep Plan Maintenance, the more existence of good and effective business continuity and disaster recovery plan.

For Business Continuity/Disaster Recovery Plan Testing, Auditing, and Maintenance, the spearman correlation coefficient equals 0.872 which means that there is a significant relationship between Business Continuity/Disaster Recovery Plan Testing, Auditing, and Maintenance and the seven components.

This means that the more existence of accurate and deep plan Testing, Auditing, and Maintenance, the more existence of good and effective business continuity and disaster recovery plan.

For Business Continuity/Disaster Recovery Training, the spearman correlation coefficient equals 0.721 which means that there is a significant relationship between Business Continuity/Disaster Recovery Training and the seven components

This means that in order to increase the level of existence of good and effective BC/ disaster recovery plan, a well designed and monitored training should be conducted by companies.

It was concluded from the high correlation of all 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 component 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, and business impact analysis.

This result agrees with significant prior research:

1. (Kon, 1997): The study reported that business continuity planning has to compromise the following components:

    - Obtain top management approval and support.
    - Perform business impact analyses.
    - Evaluate critical needs and prioritize business requirements.
    - Determine the business continuity strategy and associated recovery process.
    - Test the business recovery process and evaluate test results.
    - Develop and review service level agreement(s).
    - Update and revise the business recovery procedures and templates.

6.2.3. The Third hypothesis:

"There is no significant difference among respondents regarding to the application of Business Continuity and Disaster Recovery plan to the following independent variables: Job Title. Qualification. Experience. Age. Company size. Number of information technology staff."

Statistical hypothesis tests:

- Mann-Whitnay test to examine if there is a statistical significant difference among respondents regarding to the application of Business Continuity and Disaster Recovery due to personal traits (Job Title. Qualification. Experience. Age. Company size. Number of information technology staff)
- The Kruskal-Wallis test is used to check and if there are any significant difference among respondents regarding to the application of Business Continuity and Disaster Recovery due to personal traits (Job Title. Qualification. Experience. Age. Company size. Number of information technology staff).

Hypothesis:

There is no significant difference among respondents regarding to the application of Business Continuity and Disaster Recovery due to personal traits (Job Title. Qualification. Experience. Age. Company size. Number of information technology staff).

This hypothesis can be divided into the following sub-hypotheses:

1- There is no significant difference among respondents regarding to the application of Business Continuity and Disaster Recovery due to Qualification.

Table (6.14) shows that the p-value (Sig.) is greater than the level of significance $\alpha = 0.05$ for each field, then there is insignificant difference among the respondents regarding to the application of Business Continuity and Disaster Recovery due to Qualification.

It was concluded that the respondents' Qualification has no effect on the application of Business Continuity and Disaster Recovery.

This is due to the fact that these skills and knowledge are not taught in the universities, these skills are acquired by the real practice, experience, and work conditions.

So it is reasonable and logic that the qualification has no effect on the application of the plan.

Table (6.14): Mann-Whitney test of the fields and their p-values for Qualification

Field	Test value	P-value(Sig.)
Project Initiation	-0.841	0.400
Risk Assessment	-1.176	0.240
Business Impact Analysis	-1.311	0.190
Mitigation Strategy Development	-0.650	0.516
Business Continuity/Disaster Recovery Plan Development	-1.588	0.112
Business Continuity/Disaster Recovery Plan Testing	-0.448	0.654
Business Continuity/Disaster Recovery Plan Auditing	-0.740	0.460
Business Continuity/Disaster Recovery Plan Maintenance	-0.848	0.396
Business Continuity/Disaster Recovery Plan Testing, Auditing, and Maintenance	-0.839	0.402
Business Continuity/Disaster Recovery Training	-1.055	0.291
All Seven components	-1.206	0.228

2- There is no significant difference among respondents regarding to the application of Business Continuity and Disaster Recovery due to Job Title.

Table (6.15) shows that the p-value (Sig.) is greater than the level of significance $\alpha = 0.05$ for each field, then there is insignificant difference among the respondents regarding to the application of Business Continuity and Disaster Recovery due to Job Title.

It was concluded that the respondents' Job Title has no effect on the application of Business Continuity and Disaster Recovery.

This is due to the fact that plan application is not personal tendencies, but it is company orientations. So there were no differences in the answers of respondents regarding their titles, because the driver behind that was the company culture.

Table (6.15): Kruskal-Wallis test of the fields and their p-values for Job Title

Field	Test Value	Df*	Sig.
Project Initiation	0.201	2	0.904
Risk Assessment	0.220	2	0.896
Business Impact Analysis	0.777	2	0.678
Mitigation Strategy Development	3.853	2	0.146
Business Continuity/Disaster Recovery Plan Development	2.220	2	0.330
Business Continuity/Disaster Recovery Plan Testing	0.176	2	0.916
Business Continuity/Disaster Recovery Plan Auditing	0.291	2	0.865
Business Continuity/Disaster Recovery Plan Maintenance	0.716	2	0.699
Business Continuity/Disaster Recovery Plan Testing, Auditing, and Maintenance	0.546	2	0.761
Business Continuity/Disaster Recovery Training	0.073	2	0.964
All Seven components	0.131	2	0.937

* df : Degrees of Freedom

3- There is no significant difference among respondents regarding to the application of Business Continuity and Disaster Recovery due to Specialization.

Table (6.16) shows that the p-value (Sig.) is smaller than the level of significance $\alpha = 0.05$ for each field, then there is significant difference among the respondents regarding to the application of Business Continuity and Disaster Recovery due to Specialization.

It was concluded that the respondents' Specialization has an effect on the application of Business Continuity and Disaster Recovery.

Table (6.16): Kruskal-Wallis test of the fields and their p-values for Specialization

Field	Test Value	df	Sig.
Project Initiation	8.259	2	0.016*
Risk Assessment	8.678	2	0.013*
Business Impact Analysis	10.296	2	0.006*
Mitigation Strategy Development	6.812	2	0.033*
Business Continuity/Disaster Recovery Plan Development	10.793	2	0.005*
Business Continuity/Disaster Recovery Plan Testing	7.789	2	0.020*
Business Continuity/Disaster Recovery Plan Auditing	13.456	2	0.001*
Business Continuity/Disaster Recovery Plan Maintenance	11.299	2	0.004*
Business Continuity/Disaster Recovery Plan Testing, Auditing, and Maintenance	12.652	2	0.002*
Business Continuity/Disaster Recovery Training	12.834	2	0.002*
All Seven components	14.345	2	0.001*

* Means differences are significant at $\alpha = 0.05$

Table (6.17) shows the mean rank for each Specialization. It was concluded From table (6.17), the following:

For each component all the seven components together, Computer Engineer's respondents have the highest mean among the other Specialization toward the application of Business Continuity and Disaster Recovery.

This is due to the fact that the specialization forms part of the personal character, and most of engineers are actually pioneers in their jobs and life. This is in addition to that most of engineering university departments give their students management courses, and researched topic is a combination between the management(planning) and technical (information technology). So it is expected that the engineers are the nearest ones to this mixture.

Table (6.17): Mean rank for each Specialization

Field	Mean Rank		
	Computer Engineer	**Computer science**	**Business Administration**
Project Initiation	36.69	25.63	21.55
Risk Assessment	33.96	23.93	19.15
Business Impact Analysis	33.65	26.28	15.20
Mitigation Strategy Development	33.69	21.95	23.75
Business Continuity/Disaster Recovery Plan Development	35.17	22.15	19.80
Business Continuity/Disaster Recovery Plan Testing	32.17	27.40	16.50
Business Continuity/Disaster Recovery Plan Auditing	33.58	27.68	12.55
Business Continuity/Disaster Recovery Plan Maintenance	33.56	26.95	14.05
Business Continuity/Disaster Recovery Plan Testing, Auditing, and Maintenance	34.27	26.38	13.50
Business Continuity/Disaster Recovery Training	36.02	26.18	15.55
All Seven components	38.90	25.27	17.10

4- There is no significant difference among respondents regarding to the application of Business Continuity and Disaster Recovery due to Experience.

Table (6.18) shows that the p-value (Sig.) is greater than the level of significance $\alpha = 0.05$ for each field, then there is insignificant difference among the respondents regarding to the application of Business Continuity and Disaster Recovery due to Experience**.**

It was concluded that the respondents' experience has no effect on the application of Business Continuity and Disaster Recovery.

This is due to fact that the researched topic is considered as modern topic, and the experience of the respondents did not affect the application of planning.

Table (6.18): Kruskal-Wallis test of the fields and their p-values for Experience

Field	Test Value	df	Sig.
Project Initiation	1.456	3	0.693
Risk Assessment	1.562	3	0.668
Business Impact Analysis	3.148	3	0.369
Mitigation Strategy Development	1.450	3	0.694
Business Continuity/Disaster Recovery Plan Development	1.005	3	0.800
Business Continuity/Disaster Recovery Plan Testing	1.162	3	0.762
Business Continuity/Disaster Recovery Plan Auditing	1.969	3	0.579
Business Continuity/Disaster Recovery Plan Maintenance	1.823	3	0.610
Business Continuity/Disaster Recovery Plan Testing, Auditing, and Maintenance	2.450	3	0.484
Business Continuity/Disaster Recovery Training	3.974	3	0.264
All Seven components	0.361	3	0.948

5- There is no significant difference among respondents regarding to the application of Business Continuity and Disaster Recovery due to Age.

Table (6.19) shows that the p-value (Sig.) is greater than the level of significance $\alpha = 0.05$ for each field, then there is insignificant difference among the respondents regarding to the application of Business Continuity and Disaster Recovery due to Age.

It was concluded that the respondents' Age has no effect on the application of Business Continuity and Disaster Recovery.

This is due to fact that the researched topic is considered as a modern topic, and the age of the respondents did not affect the application of planning.

Table (6.19): Mann-Whitney test of the fields and their p-values for Age

Field	Test value	P-value(Sig.)
Project Initiation	-1.028	0.304
Risk Assessment	-1.665	0.096
Business Impact Analysis	-0.751	0.453
Mitigation Strategy Development	-1.647	0.100
Business Continuity/Disaster Recovery Plan Development	-0.065	0.948
Business Continuity/Disaster Recovery Plan Testing	-0.886	0.376
Business Continuity/Disaster Recovery Plan Auditing	-1.069	0.285
Business Continuity/Disaster Recovery Plan Maintenance	-0.774	0.439
Business Continuity/Disaster Recovery Plan Testing, Auditing, and Maintenance	-0.871	0.384
Business Continuity/Disaster Recovery Training	-0.228	0.819
All Seven components	-0.649	0.516

Chapter Seven:
Conclusion and Recommendations

Preface:

After presenting and discussing the findings of the research, this chapter discuses the key findings and recommendations that the researcher suggests to enhance and promote the strengths and effectiveness of the business continuity and disaster recovery plans.

This chapter will discuss the following two main issues:

1. Conclusion
2. Recommendations
3. Future Work

7.1. Conclusion

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 Palestinian listed companies, but up to now there were shortages in some components of the plan. This is a high risky situation, because as revealed from the analysis in the last chapter, the majority of the companies 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 targedted companies 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 respondants 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 Palestinian companies consider as large companies, so it has to apply business continuity and disaster recovery planning in their businesses, companies diverse in introducing information technology services in targeted companies, Companies depends mainly on information technology services, but actually there were also the lack of spatiality inside information technology departments. Companies were diverse in the size and type of information technology services introduced to companies, but 58.1% less than 3 workers actually indicates weaknesses in the human resource requirements in information technology department in the targeted companies.

Data compiled also revealed that (54.8%) of respondents' companies 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 companies 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 companies 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 of weak 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 companies 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 companies.

(82.81%) of the Mitigation Strategies were found, It means that the majority of the targeted companies 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 companies had good skills and experience in such field. Moreover most of companies can provide the required materials and equipments 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 companies' 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 companies. While the P-Value more than 5%, it reflected that the targeted companies did not agree to a unified and similar answer in developing their plan. This was due to the fact that not all of companies had written their plan and not all of the companies had such plans, which reflect a weakness in writing the plans in some of companies.

It was concluded that plan testing, auditing, and maintaining procedures applied in the targeted companies 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 companies 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 companies.

Testing, auditing, maintaining, and training procedures were followed, but companies 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 companies 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 the sig. 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.

7.2. 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:

1. Companies are advised to give more concern to Project Initiation techniques.
2. Companies are advised to give more concern to Risk Assessment.
3. Companies are advised to give more concern to Business Impact Analysis.
4. Companies are advised 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.
5. Companies are advised to spend more efforts in amending the Plan Development.
6. Companies are advised to enhance their practicing toward Plan Maintenance.
7. Companies are advised to enhance their practicing toward Plan Auditing.
8. Companies are highly advised to adopt business continuity and disaster recovery plans according to the suggested model in this study.
9. Palestinian authority is advised to prepare a law to mandate Palestinian companies to prepare their own business continuity and disaster recovery plans according to such this model suggested in this study.
10. Companies are advised to train their employees to collaborate with researchers, and to enhance scientifical research culture between their employees.
11. University library manager is advised to enrich the library with references related to the topic of research.
12. Arabs researchers are encouraged to take procedures in applying such research to their areas companies.

7.3. Future Work

1. Researchers are advised to apply further researches on companies in Palestine by studying the seven components of business continuity and disaster recovery plans in more details.
2. Researchers are advised to apply this field of research on others sectors such as: governmental ministries, and higher education institutes.

BIBLIOGRAPHY

- Al-Badi Ali H., Ashrafi Rafi, Al-Majeeni Ali O., Pam J. Mayhew,(2009),"information technology disaster recovery: Oman and Cyclone Gonu lessons learned". Information Management & Computer Security, Year: 2009 Volume: 17 Issue: 2Publisher: Emerald Group Publishing Limited.
- Andrews, W. C. (1990). "Contingency Planning For Physical Disasters." Journal of Systems Management 41(7): 28-32.
- AT&T,(2007), available at "http://www.att.com/Common/merger/files/pdf/business_continuity_07/Business_Continuity_Study_Results.pdf."(Accessed 29 Oct. 2008).
- Bajgoric Nijaz ,(2005), "Information systems for e-business continuance: a systems approach", Kybernetes, Volume: 35 Issue: 5,Emerald Group Publishing Limited.
- Bandyopadhyay Kakoli ,(2001), "The role of business impact analysis and testing in disaster recovery planning by health maintenance organizations" ,Hospital Topics; Winter 2001; 79, 1.
- Bandyopadhyay Kakoli, (2002),"Disaster-preparedness of health maintenance organizations",Disaster Prevention and Management; 2002; 11, 4; ABI/INFORM Global.
- Barbara, Michael, (2006) “Determining the Critical Success Factors of an effective Business Continuity / Disaster Recovery Program in a Post 9/11 World: a Multi-Method Approach.”, M. B. A Thesis, Concordia University.
- Botha Jacques and Von Rossouw,(2004), "A cyclic approach to business continuity planning",Information Management & Computer Security; 2004; 12, 4; ABI/INFORM Global.
- Botha, J. and R. Von Solms, (2004). “A Cyclic Approach to Business Continuity Planning.” Information Management & Computer Security
- Brandon,(2006), " Project management for modern information systems",IRM,ISBN 1-59140-694-3.
- Business Continuity Institute ,(2006),A Management Guide to Implementing Global Good Practice in Business Continuity Management.
- Canon D.,Bergmann T.,and Pamplin,(2006)," Certified Information Systems Auditor",Wiley,ISBN-13: 978-0-7821-4438-3.

- Carvajal-Vion, J.-F. and M. Garcia-Menendez, (2003). "Business Continuity Controls in ISO 17799 and COBinformation technology." Upgrade: European Journal for the Informatics Professional 4(6): 17-23.
- Castillo, C., (2004). "Disaster Preparedness and Business Continuity Planning at Boeing: an Integrated Model." Journal of Facilities Management 3(1): 8-26.
- Cerullo Virginia and Michael J Cerullo,(2004),"Business continuity planning: a comprehensive approach",Information Systems Management; Summer 2004; 21, 3; ABI/INFORM Global.
- Cerullo, V. and M. J. Cerullo, (2004). "Business Continuity Planning: A Comprehensive Approach." Information Systems Management 21(3): 70-78.
- Cervone H. Frank,(2006),"Disaster recovery and continuity planning for digital library systems",OCLC systems & Services, Emerald Group Publishing Limited, Volume: 22, Issue: 3.
- Chow, W. S. (2000). "Success Factors for IS Disaster Recovery Planning in Hong Kong." Information Management & Computer Security
- Dalmadge Creston, (2001), "A method for measuring the risk of e-business discontinuity",Doctorate Dissertation, College of Business Administration, Southern illinois University,Carbondale,USA.
- Deepak Kumer Gupta,(2003) ,"An Analysis of the Disruptions in the U.S Apparel Manufacturing Industry and Identification of Continuity Planning Strategies",Master's Thesis,unrestricted.
- DRI International, (2006). "Professional Practices for Business Continuity Professionals", DRI International. 2006.
- Elliott, D., E. Swartz, et al. (1999). "Just Waiting for the Next Bang: Business Continuity Planning in the UK Finance Sector." Journal of Applied Management Studies 8(1): 43¬60.
- Ernest Jordan,(1996),"information technology contingency planning: management roles", Information Management & Computer Security. Bradford 1999. Vol. 7, Iss. 5.
- Gallagher M.,(2003),"Business Continuity Management", Prentice Hall ,ISBN 0 273 66351 8.
- Greer Gregg,(2003), "Higher Education Business Continuity Survey" ,Master Thesis, Baylor University, Waco, Texas, USA.
- Grillo, A., (2003). "Information Systems Auditing of Business Continuity Plans." European Journal for the Informatics Professional 4(6): 12-16.
- Hawkins, S. M., D. C. Yen, et al. (2000). "Disaster Recovery Planning: a Strategy for Data Security." Information Management & Computer Security. 8(5): 222-229.

- Heathfield Susan,(2009),"What Is the Human Resource Department",available at "http://humanresources.about.com/od/glossaryh/f/hr_department.htm."(accessed 21 Oct. 2008).
- Hood, S. B., (2005). "Always Be Prepared: 10 Ways to Know if You're Ready for Any Disaster", Canadian Business: 3.
- Information Technology Association of America (information technologyAA), (2008) "Information Technology Definition."
- information technologyTA, (2008),"Information Technology:Creating Added Value Across Public Transport Networks", available at: http://www.uitp.org/news/pics/pdf/MB_information technology_final.pdf (Accessed 20 Aug. 2008).
- Iyer, R. J. and K. Bandyopadhyay,(2000), "Managing Technology Risks in the Healthcare Sector: Disaster Recovery and Business Continuity Planning." Disaster Prevention and Management 9(4): 257-267.
- Jackson, Richard ,(2006), "Business continuity: preparation over prevention.(information technology Systems) ", Accountancy Ireland ,Article.
- Jacobs, J. and S. Weiner (1997). "The CPA's Role in Disaster Recovery Planning." The CPA Journal 67(11): 20-25.
- Jolly A., (2003),"The Secure Online Business", Kogan Page Limited,ISBN 0 7494 3936.
- Jordan, E. (1999). "information technology Contingency Planning: Management Roles." Information Management & Computer Security.
- Karakasidis, Kon.,(1997), "A project planning process for business continuity", Information Management & Computer Security. Bradford: 1997. Vol. 5, Iss. 2.
- Laudon K. and J. laudon, (2006),Management Information Systems: Managing the Digital Firm, 9/e.,Pearson Prentice Hall , ISBN 9780136078463].
- Lennon E., (2002),"contingency planning guide for information technology systems".
- Lumpur Kuala, (2007),"Business continuity, disaster recovery awareness high", Malaysian Business,Periodical,01265504.
- Lumpur, Kuala (2007) "Business continuity, disaster recovery awareness high." Malaysian Business.
- Marianne Swanson, Amy Wohl, Lucinda Pope, Tim Grance, Joan Hash, Ray Thomas,(2002) Contingency Planning Guide for Information Technology Systems,NIST,U.S. Government Printing Office.

- Marianne Swanson, Amy Wohl, Lucinda Pope,Tim Grance, Joan Hash, Ray Thomas,(2006),Contingency Planning Guide for Information Technology Systems,NIST,U.S. Government Printing Office.
- McCracken, A. (2005). Unravelling Business Continuity Terminology, Continuity Central.
- Moh Heng, Goh,(1996), "Developing a suitable business continuity planning methodology",Information Management & Computer Security. Bradford: 1996. Vol. 4, Iss. 2;
- Moore, D., McCabe, G., Duckworth, W., Sclove, S., 2003, "The Practice of Business Statistics".
- Morwood Gregory,(1998), "Business continuity: awareness and training programmes", Information Management & Computer Security. Bradford: 1998. Vol. 6, Iss. 1.
- Noakes K., 2001, "Business Continuity and Disaster Recovery Planning and Management: Perspective, Trude Diamond."
- Palestinian security exchange (PSE), 2008,"Breif history", available at: "http://212.14.224.121/PSEWEB/Forms/en/AboutUsHistory.aspx" (accessed 21 February 2008).
- Pat. Moore,(1995),"Critical elements of a disaster recovery and business/service continuity plan" , Facilities. Bradford: Aug 1995. Vol. 13, Iss. 9,10.
- 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.
- Ramesh P., (2002), "Business Continuity Planning", Tata.
- Rohde, R. and J. Haskett (1990). "Disaster Recovery Planning for Academic Computing Centers." Communications of the ACM 33(6): 652-657.
- Ronald L. KrutzandRussell Dean Vines,(2007),"The CISSP and CAP Prep Guide",John Wiley & Sons ,ISBN:9780470007921.
- Savage, M. (2002). "Business Continuity Planning." Work Study 51(4/5):254-261.
- Scott, Karen (2006) "Strategic contingency planning.", Master of Science in emergency services administration Thesis, California State University.
- Sharon. Cunningham, (1988),"Developing a Disaster Recovery Plan (Disaster recovery planning) Using a Data Base Package", Computers & Industrial Engineering. New York: 1988. Vol. 15, Iss. 1-4;

- Smith, R. (1995). "Business Continuity Planning and Service Level Agreements." Information Management & Computer Security 3(3): 17-21.
- Snedaker, Susan (2007) “Business Continuity & Disaster Recovery for information technology Professionals.” Syngress Publishing.
- Stoneburner, Gary, Goguen, Alice, and Feringa, Alexis,(2001),"Risk Management Guide for Information Technology Systems", National Institute of Standards and Technology, Publication 800-30.
- Tatum Malcolm,(2009),"What is an information technology Department? ,available at "http://www.wisegeek.com/what-is-an-it-department.htm",accessed(20 Sep. 2009).
- Tayeh Alaiddin,(2008),“Effectiveness of Information "Security Management at the Palestinian Information Technology Companies” ,published , Master Thesis, Islamic University of Gaza,Palestine.
- Wikipedia, (2008) “Information system” available at: “http://en.wikipedia.org/wiki/Information_system” (accessed 21 February 2008).
- Williamson Bob.,(2007), "Trends in business continuity planning: in business continuity planning, financial organizations are ahead of other types of businesses.
- Wilson B. (2000), “Business continuity planning: a necessity in the new e-commerce era”, Disaster Recovery journal, available at: “www.drj.com/articles/fa100/1304-02.htm” (accessed 21 Feb. 2009).
- Wong Bo K; Monaco, John A; andSellaro, C Louise, (1994)., "Disaster recovery planning: Suggestions to top management and information systems managers", Journal of Systems Management; May 1994; 45, 5; ABI/INFORM Global
- Zsidisin George Ragatz,Gary and Steven Melnyk,(2003),"Effective Practices in Business Continuity Planning for Purchasing and Supply Management", Research paper, Michigan State University, USA.

Appendices

1. English Questionnaire

Part1
General Information

a) Personal Profile: Please indicate X in the correct answer.

1. Qualification :
☐ Diploma ☐ Bachelor ☐ Master ☐ Doctorate

2. Job Title:
☐ Manager ☐ Supervisor ☐ Engineer/programmer/Developer ☐ Technical ☐ others

3. Specialization:
☐ Computer Engineer ☐ Computer science ☐ Business Administration ☐ others

4. Experience
☐ Less than5 years ☐ 5-10years ☐ 11-15year ☐ more than 15 years

5. Age
☐ Less than 25 ☐ 25-35 ☐ 35-45 ☐ Elder than 45

b) Company Profile: Please indicate X in the correct answer.

6. Number of workers in the company:
☐ <10 ☐ 10-50 ☐ 51-100 ☐ >100

7. Company Type:
☐ Industrial ☐ Trading ☐ Service ☐ Others

8. Information technology Services done by:
☐ Internal Department ☐ Outsourcing ☐ Mixed

9. Information technology Department Sections:
☐ 1 ☐ 2 ☐ 3 ☐ more than 3

10. Number of employees in information technology department
☐ Less than 3 ☐ 3-5 ☐ 6-10 ☐ More than 10

Part2

Business Continuity and Disaster Recover

a) Disaster Types:

1	**Has your company ever faced a disaster threats?**	**Yes**	☐	**No**	☐
2	**IF yes, what is the disaster type?**	**Human Caused**	☐	**Infrastructure Threat**	☐
		Others			☐
3	**Disaster strikes**	**Hardware**	☐	**Software**	☐
		Staff	☐	**Others**	☐

Part3

The basic steps in Business continuity and disaster recovery plan

Set an estimate answer from 1-10, 1 indicates a weak answer while 10 indicates a strong answer.

The basic Components of Business continuity and disaster recovery plan		
1) Project Initiation		**1-10**
1.	Your plan contains project management techniques such as task management, resource allocation and budgeting.	
2.	Plan is supported from top management.	
3.	Employees are involved in setting the plan.	
4.	Experience Project manager Leads the team.	
5.	Plan Objectives are clear.	
6.	Plan requirement are well defined.	
7.	Plan scope and schedule are clear.	
2) Risk Assessment:		
1.	Risk assessment phase of Business continuity and disaster recovery provides management with the necessary information to further evaluate or analyze each identified threat.	
2.	Risk assessment phase of Business continuity and disaster recovery considers all possible threats to the IS, such as natural disaster, hardware and software failure, and human error.	
3.	Risk assessment phase of Business continuity and disaster recovery identifies specific threats to business operations and measures each one's probability of	

	occurrence.	
4.	Risk assessment phase of Business continuity and disaster recovery discovers a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised.	
5.	In risk assessment, information is collected about, Hardware, Software, System interfaces, Data and information, and System and data criticality.	
3) Business Impact Analysis		
1.	During business impact analysis phase, critical business processes are identified and then analyzed.	
2.	Business impact analysis helps the organization to understand the degree of potential loss which could occur.	
3.	Your plan has a category system with all rating systems, the categories are clearly defined, and that there is a shared understanding of the proper use and scope of each.	
4.	Business impact analysis informs a management decision on Maximum Tolerable Outage for each function, Maximum Tolerable Downtime Recovery Time Objective.	
4) Mitigation Strategy Development		
1.	Your mitigation strategy contains development of strategies to accept, avoids, reduce, or transfer risks related to potential business disruptions.	
2.	Your mitigation strategy covers critical data and records, to ensure that all critical information, activities, systems, and material is properly backed up and stored off-site	
3.	Your mitigation strategy covers critical systems and Infrastructure, to evaluate hardware and software solutions, vendors, and costs.	
4.	Your mitigation strategy covers information technology recovery systems, to grantee that all mission-critical information and equipment are appropriately safeguarded from any possible loss or damage. This full recovery strategy includes preliminary measures, descriptive recovery procedures, selection of an appropriate backup site and detail of backup and off-site storage requirements of vital information and equipment. • Alternate Sites • Fully Mirrored Site	

	• Hot Site • Warm Site • Cold Site	
5.	Your mitigation strategy covers information technology backup Systems such, Disk Systems Disk systems solutions continue to evolve in terms of capabilities RAID Data backup strategy Full backup Incremental method Differential method	
6.	Your mitigation strategy covers anthers solutions such as: Remote Journaling: Remote journaling refers to the parallel processing of transactions to an alternate site. And Replication: Disk replication involves copying data on to a primary and secondary server.	
7.	Your mitigation strategy takes in account Standby Operating Systems.	
8.	Your mitigation strategy takes in account Desktop Solutions and user data.	
9.	Your mitigation strategy takes in account backing up and storing Software and Licensing at an offsite storage location.	
10	Your mitigation strategy takes in account backing up and storing Web Sites through Load balancing strategies to ensure Web sites have high availability. Document Web Site. Web Site Programming. Web Site Coding.	
5) Business Continuity/Disaster Recovery Plan Development		
1.	In plan development you take mitigation strategies and identify methods for implementing those strategies, people, resources, and tasks needed to complete these activities	
2.	In plan development you state 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	
3.	In plan development you define communications plan to control the communication while a disaster occurred.	

4.	In plan development you define the initial actions taken once a system disruption or emergency has been detected.	
6) Business Continuity/Disaster Recovery Plan Testing, Auditing, and Maintenance.		
Business Continuity/Disaster Recovery Plan Testing		
1.	Plan is tested on a periodic and regular basis.	
2.	The Business continuity and disaster recovery plan should be exercised at least annually.	
3.	Plan testing determines whether the right resources have been identified	
4.	Plan testing identifies gaps or weaknesses in the plan.	
Business Continuity/Disaster Recovery Plan Auditing		
1.	Plan auditing is done to ensure information technology risk mitigation strategies are in place and properly implemented/configured.	
2.	Plan auditing is done to ensure systems identified by the Business continuity and disaster recovery plan are still in place and functioning.	
3.	By auditing data reviewed regarding various systems to ensure they are still compliant with the Business continuity and disaster recovery plans.	
Business Continuity/Disaster Recovery Plan Maintenance		
1.	The plan use a revision numbering system, so team members know whether they have the latest version of the plan.	
2.	Key contact information are revised, reviewed, and updated regularly.	
3.	There are up-to-date copies of the Business continuity and disaster recovery plan off-site in the event the building is inaccessible.	
4.	Plan maintenance procedures are Documented, to avoid introducing additional risk into the project.	
7)Business Continuity/Disaster Recovery Training		
1.	Staff is well trained on the plan activation and treatment.	
2.	Company performs training needs assessment to fill the gaps in skills.	
3.	Plan Training identified the training Scope, Objectives, Timelines, and Requirements.	
4.	Company finds various training programs online that people can attend on their own schedule.	
5.	Training Monitoring is done to ensure key personnel have actually attended required training.	

2. Arabic Questionnaire

الجامعة الإسلامية- غزة
عمادة الدراسـات العليا
ماجسـتير إدارة الأعـمال

السيد : _____ المحترم

السلام عليكم ورحمة الله وبركاته...

الموضوع / استبانه لبحث ماجستير في إدارة الأعمال

مرفق لسيادتكم طيه استبانه يهدف الباحث من خلالها إلى تقيم التخطيط لاستمرار العمل والاسـتعادة مـن الكوارث(خطة الطوارئ) في أقسام تكنولوجيا المعلومات في الشركات المدرجة في سوق فلسطين للاـسوق المـالي، وذلك استكمالاً لمتطلبات الحصول على درجة الماجستير في إدارة الأعمال، وقد تم تصميم الإستبانه بغرض جمـع البيانات التي تساعد في إتمام هذا البحث تحت عنوان:

تقيم التخطيط لاستمرار العمل والاستعادة من الكوارث(خطة الطوارئ) في أقسام تكنولوجيا المعلومات في الشركات المدرجة في سوق فلسطين للأوراق المالية

وعليه نرجو من سيادتكم الإجابة على الإستبانه حيث أن مساهمتكم سيكون لها أبلغ الأثر في نجـاح البحـث ودقـة نتائجه.

وتقبلوا بقبول فائق الاحترام والتقدير والشكر على المساعدة ،،،،،

الباحث

محمد إنشاصي

0598913093

القسم الأول

أولاً: (السمات الشخصية): ضع علامة (X) أمام الإجابة الصحيحة:

1- المؤهل العلمي:-

☐ دبلوم ☐ بكالوريوس ☐ ماجستير ☐ دكتوراه

2- مسمى الوظيفة:-

☐ مدير دائرة ☐ رئيس قسم

☐ مهندس / مبرمج / مطور ☐ فني ☐ أخرى حدد .....

3- التخصص العلمي:-

☐ هندسة حاسوب ☐علوم حاسوب ☐ إدارة أعمال ☐ أخرى حدد .....

4- سنوات الخبرة:-

☐ اقل من 5 سنوات ☐ من 5 إلى 10 سنوات ☐من 11 إلى 15 سنة ☐ أكثر من 15 سنة

5- العمر:-

☐ أقل من 25 ☐ 25- 35 ☐ 36- 45 ☐ أكثر من 45

ثانيا – معلومات عامة:-

1- إجمالي عدد العاملين بالشركة:-

☐ أقل من 10 ☐ من 10 - 50 ☐ من 51 – 100 ☐أكثر من 100

2- نوع نشاط الشركة:-

☐ صناعي ☐ تجاري ☐خدماتي ☐ أخرى حدد .....

3- خدمات تكنولوجيا المعلومات في الشركة يقوم بها:-

☐ قسم داخلي ☐ جهات خارجية ☐ خليط ما بين الاثنين

4- عدد أقسام تكنولوجيا المعلومات في الدائرة:-

☐ قسم واحد ☐ قسمان ☐ ثلاثة أقسام ☐ أكثر من ثلاثة أقسام

5- عدد الموظفين في دائرة تكنولوجيا المعلومات:-

☐ أقل من 3 موظفين ☐ من 3- 5 موظفين ☐ من 6- 10 موظفين ☐ أكثر من 10 موظفين

الجزء الثاني: أنواع الكوارث التي تعرضت لها شركتكم

1	هل سبق وأن تعرضـت شـركتك لحوادث كارثية (مشكلة) ؟	☐ نعم		☐ لا	
2	إذا كانت الإجابة نعم مـا سـبب الكارثة (المشكلة) التي تعرضـت لها شركتكم؟	☐ صنع بشري	☐ تكنولوجي	☐ انهيار في البنية التحتية	☐ غير ذلك حدد.....
3	الكارثة(المشكلة) أصابت	☐ عتاد الحاسوب Hardware	☐البرمجيات Software	☐ الطاقم Staff	☐ غير ذلك حدد.....

الجزء الثالث: ضع تقديرا من (1-10) بحيث أن 1 تدل على سلبية قوية للإجابة و10 تدل علـى ايجابيـة قويـة للإجابة.

الخطوات الهامة لخطة استمرار العمل والاستعادة من الكوارث(خطة الطوارئ)		**10-1**
1. أساسيات إعداد خطة استمرار العمل والإستعادة من الكوارث(خطة الطوارئ)		
م.	**البيان**	
.1	لديك خطة تحتوي على أساسيات إدارة المشروع، مثل تحديد المهام، وتخصيص الموارد، وعمـل الموازنة.	
.2	الخطة مدعومة من الإدارة العليا.	
.3	شارك العاملون في إعداد الخطة.	
.4	يتم إعداد وتطبيق الخطة من قبل فريق عمل يرأسه مختص.	
.5	الاحتياجات المادية والبشرية للخطة محددة بشكل جيد.	
.6	الاحتياجات المادية والبشرية للخطة متوفرة بشكل جيد.	
.7	أنشطة وجداول العمل محددة في جداول زمنية واضحة.	
2. تقدير المخاطر		
.1	يتم تقدير المخاطر لديكم، وهذا يزود الإدارة بالمعلومات اللازمة لتقييم وتحديد الأخطار للشركة.	
.2	يتم التعامل مع كل الأخطار المحددة بنظم المعلومات لديكم. **Hardware, software failure, and human error**	
.3	يتم تقدير مستوى الأخطار لعمليات الشركة، ويتم قياس احتمال حدوث كل تهديد منها.	
.4	دراسة المخاطر لديكم تكشف مستوى الضعف في نظم الأمان.	
.5	يحتوي تقدير المخاطر لديكم على دراسة كل من : **Hardware, Software, System interfaces, and information.**	
3. تحليل أثر الخطر على المؤسسة		
.1	تقوم الشركة بتحديد وتحليل كافة العمليات الرئيسة.	
.2	يعطي تحليل أثر الخطر لديكم فهما واضحا عن الأهداف الحساسة والمهمـة للـشركة، وأولويـات	

	الشركة، والوقت الإجمالي للعودة للعمل بعد أي خطر أصابها.	
.3	يتم تصنيف الأخطار حسب درجة تأثيرها.	
.4	يتم تحديد الفترة الزمنية لتعطل العمل في أي وظيفة من وظائف المؤسسة بدقـه، وأثـر ذلـك التعطل.	
4.	**<u>إستراتجيات مواجهة الكارثة</u>**	
.1	يتم تحديد استراتيجة لمواجهة الخطر مثل: قبول الخطر، أو التقليل من حدته، أو تلافيـه، أو نقـل المخاطرة إلي طرف آخر كالتأمين.	
.2	يتم تغطية كل المعلومات والسجلات المهمة في الشركة، للتأكد من أن هذه المعلومـات والأنـشطة والأنظمة المتعلقة بها لها نسخ احتياطيه خارج المؤسسة وذلك لمواجهة أي خطر.	
.3	يتم تغطية كل أنظمة الحاسوب لديكم، لتأمين المعلومات لكل الأقسام الهامة من أي فقدان أو تلف في إستراتجية مواجهة الكوارث المتبعة عندكم.	
.4	يتم الأخذ بعين الاعتبار حلولا مناسبة من استراتيجيات حماية المعلومات والأدوات المهمة لديكم مثل : **Alternate Sites, Fully Mirrored Site, Hot Site, Warm Site, or Cold Site.**	
.5	يتم الأخذ بعين الاعتبار حلولا مناسبة من استراتيجيات النسخ الاحتياطي مثل: **RAID, Data backup strategy, Full backup, Incremental, and Differential.**	
.6	يتم الأخذ بعين الاعتبار لحلول أخرى في إستراتجية مواجهة الكوارث المتبعة عندكم مثل: **Remote Journaling and Replication.**	
.7	يتم الاحتفاظ بنظم تشغيل احتياطية لاستخدامها عند الحاجة.	
.8	يتم الاحتفاظ بنسخ احتياطية لمعلومات المستخدمين.	
.9	يتم الاحتفاظ بنسخ احتياطية لتراخيص البرمجيات لديكم خارج المؤسسة.	
.10	إستراتجية مواجهة الكوارث المتبعة لديكم تتضمن استراتجيات لحماية موقعكم على الانترنت مثل: **Load balancing, Document Web Site, Web Site Programming saving, and Web Site Coding.**	
5.	**<u>صياغة وكتابة خطة استمرار العمل والاستعادة من الكوارث(خطة الطوارئ)</u>**	
.1	تكتب استراتجيات مواجهة الكوارث، وطرق تنفيذها، ويتم تحديد الموارد اللازمة لإكمال تنفيذ هـذا النشاط عند صياغة الخطة.	
.2	تكتب المخاطر التي يمكن أن تتعرض لها الشركة، ونسبة توقع حدوثها، والضرر المتوقـع منهـا، واستراتيجة مواجهه كل خطر من هذه المخاطر في الخطة.	
.3	تحتوي خطة استمرار العمل والاستعادة من الكوارث علـى أنـشطة تفـصيلية خاصـة بمختلـف الاتصالات التي تقوم بها الشركة وقت الكارثة(المشكلة).	
.4	تحتوي خطة استمرار العمل والاستعادة من الكوارث على الأنشطة التي يجب القيام بها مباشرة بعد حدوث الكارثة(المشكلة)، وبعد الانتهاء منها أيضا.	
6.	**<u>اختبار وتدقيق وصيانة خطة استمرار العمل والاستعادة من الكوارث(خطة الطوارئ)</u>**	
	<u>اختبار خطة استمرار العمل والاستعادة من الكوارث(خطة الطوارئ)</u>	

1.	يتم اختبار الخطة بشكل دوري.	
2.	يتم اختبار كل عام على الأقل.	
3.	يتم اختبار موارد الخطة ودرجة كفايتها,	
4.	يحدد اختبار الضعف والفجوات الموجودة في الخطة.	
	تدقيق خطة استمرار العمل والاستعادة من الكوارث(خطة الطوارئ)	
1.	يشمل تدقيق الخطة على التأكد من أن كل استراتيجيات المواجهة فعالة وفي مكانها الصحيح.	
2.	يشمل تدقيق الخطة على التأكد من أن كل الأنظمة لا تزال تعمل في مكانها.	
3.	يشمل تدقيق الخطة على التأكد من أن البيانات والمعلومات في لا تزال صحيحة.	
	تعديل خطة استمرار العمل والاستعادة من الكوارث(خطة الطوارئ)	
1.	يوجد نظام أرشفة مناسب يضمن الرجوع إلي الخطة المحدثة.	
2.	تراجع وتعدل المؤسسة المعلومات الخاصة بالأشخاص المحورين المسئولين عن تنفيذ الخطة.	
3.	تحتفظ المؤسسة بنسخ احتياطية من الخطة المحدثة والمعدلة خارج المؤسسة.	
4.	يتم توثيق خطوات تعديل الخطة.	
7.	**التدريب على خطة استمرار العمل والاستعادة من الكوارث(خطة الطوارئ)**	
1.	يوجد فريق مدرب جيداً على تفعيل واستخدام الخطة.	
2.	يتم تدريب فريق العمل لديها بناء على الاحتياجات التدريبية لهم.	
3.	التدريب محدد المجال والأهداف والوقت والمتطلبات.	
4.	يتم توفير التدريب المناسب لكل عامل في الفريق، وكل حسب جدولة خاصة.	
5.	يتم مراقبة التدريب للتأكد من أن المتدربين يتلقوا التدريب المناسب.	

3. Referees who judged the reliability of the questionnaire

- **Dr. Rushdy Wady**
- **Dr. Samir Safi**
- **Eng. Mohammed Abu Zaeda (Master Computer Eng.)**

4. Professional Models for Business Continuity Professionals

a. Disaster Recovery Information International Model (DRII)

1. Project Initiation and Management

Establish the need for a Business Continuity Management Process or Function, including resilience strategies, recovery objectives, business continuity and crisis management plans and including obtaining management support and organizing and managing the formulation of the function or process either in collaboration with, or as a key component of, an integrated risk management initiative.

2. Risk Evaluation and Control

Determine the events and external surroundings that can adversely affect the organization and its resources (facilities, technologies, etc.) with disruption as well as disaster, the damage such events can cause, and the controls needed to prevent or minimize the effects of potential loss. Provide cost-benefit analysis to justify investment in controls to mitigate risks.

3. Business Impact Analysis

Identify the impacts resulting from disruptions and disaster scenarios that can affect the organization and techniques that can be used to quantify and qualify such impacts. Identify time critical functions, their recovery priorities, and inter-dependencies so that recovery time objectives can be set.

4. Developing Business Continuity Management Strategies

Determine and guide the selection of possible business operating strategies for continuation of business within the recovery point objective and recovery time objective, while maintaining the organization's critical functions.

5. Emergency Response and Operations

Develop and implement procedures for response and stabilizing the situation following an incident or event, including establishing and managing an Emergency Operations Center to be used as a command center during the emergency.

6. Developing and Implementing Business Continuity and Crisis Management Plans

Design, develop, and implement Business Continuity and Crisis Management Plans

that provide continuity within the recovery time and recovery point objectives.

7. Awareness and Training Programs

Prepare a program to create and maintain corporate awareness and enhance the skills required to develop and implement the Business Continuity Management Program or process and its supporting activities.

8. Maintaining and Exercising Plans

Pre-plan and coordinate plan exercises, and evaluate and document plan exercise results. Develop processes to maintain the currency of continuity capabilities and the plan document in accordance with the organization's strategic direction. Verify that the Plan will prove effective by comparison with a suitable standard, and report results in a clear and concise manner.

9. Crisis Communications

Develop, coordinate, evaluate, and exercise plans to communicate with internal stakeholders (employees, corporate management, etc.), external stakeholders (customers, shareholders, vendors, suppliers, etc.) and the media (print, radio, television, Internet, etc.).

10. Coordination with External Agencies

Establish applicable procedures and policies for coordinating continuity and restoration activities with external agencies (local, state, national, emergency responders, defense, etc.) while ensuring compliance with applicable statutes or regulations.

Taken from DRI International web site (DRI International 2006b)

b. Business Continuity Institute Model (BCI)

1. Initiation and Management

Establish the need for a Business Continuity Management Process or Function, including resilience strategies, recovery objectives, business continuity and crisis management plans and including obtaining management support and organising and managing the formulation of the function or process either in collaboration with, or as a key component of, an integrated risk management initiative.

2.. Business Impact Analysis

Identify the impacts resulting from disruptions and disaster scenarios that can affect the organisation and techniques that can be used to quantify and qualify such impacts. Identify time-critical functions, their recovery priorities, and inter-dependencies so that recovery time objectives can be set.

3. Risk Evaluation and Control

Determine the events and external surroundings that can adversely affect the organisation and its resources (facilities, technologies, etc.) with disruption as well as disaster, the damage such events can cause, and the controls needed to prevent or minimise the effects of potential loss. Provide cost-benefit analysis to justify investment in controls to mitigate risks.

4. Developing Business Continuity Management Strategies

Determine and guide the selection of possible business operating strategies for continuation of business within the recovery point objective and recovery time objective, while maintaining the organization's critical functions.

5. Emergency Response and Operations

Develop and implement procedures for response and stabilizing the situation following an incident or event, including establishing and managing an Emergency Operations Centre to be used as a command centre during the emergency.

6. Developing and Implementing Business Continuity and Crisis Management Plans

Design, develop, and implement Business Continuity and Crisis Management Plans that provide continuity within the recovery time and recovery point objectives.

7. Awareness and Training Programmes

Prepare a programme to create and maintain corporate awareness and enhance the skills required to develop and implement the Business Continuity Management Programme or process and its supporting activities.

8.Maintaining and Exercising Business Continuity and Crisis Managements Plans

Pre-plan and co-ordinate plan exercises, and evaluate and document plan exercise results. Develop processes to maintain the currency of continuity capabilities and the plan document in accordance with the organisation's strategic direction. Verify that the Plan will prove effective by comparison with a suitable standard, and report results in a clear and concise manner.

9. Crisis Communications

Develop, co-ordinate, evaluate, and exercise plans to communicate with internal stakeholders (employees, corporate management, etc.), external stakeholders (customers, shareholders, vendors, suppliers, etc.) and the media (print, radio, television, Internet, etc.).

10. Co-ordination with External Agencies

Establish applicable procedures and policies for co-ordinating continuity and restoration activities with external agencies (local, state, national, emergency responders defence, etc.) while ensuring compliance with applicable statutes or regulations.

Taken from www.thebci.org web site (BCI International)