MODULE VII

ISA

INFORMATION SYSTEMS AUDIT 2.0 COURSE

BUSINESS CONTINUITY MANAGEMENT

BACKGROUND MATERIAL

Committee on Information Technology
The Institute of Chartered Accountants of India
(Set up by an Act of Parliament)
New Delhi

Background Material
On
Information Systems Audit 2.0 Course

Module-7 Business Continuity Management (7%)

The Institute of Chartered Accountants of India
(Set up by an Act of Parliament)

New Delhi

Note: There are six other modules which form part of ISA Background Material

DISCLAIMER

The views expressed in this material are those of author(s). The Institute of Chartered Accountants of India (ICAI) may not necessarily subscribe to the views expressed by the author(s).

The information in this material has been contributed by various authors based on their expertise and research. While every effort have been made to keep the information cited in this material error free, the Institute or its officers do not take the responsibility for any typographical or clerical error which may have crept in while compiling the information provided in this material. There are no warranties/claims for ready use of this material as this material is for educational purpose. The information provided in this material are subject to changes in technology, business and regulatory environment. Hence, members are advised to apply this using professional judgement. Please visit CIT portal for the latest updates. All copyrights are acknowledged. Use of specific hardware/software in the material is not an endorsement by ICAI.

Revised Edition	:	July 2015
Committee/Department	:	Committee of Information Technology
E-mail	:	cit@icai.org
Website	:	www.icai.org/http://cit.icai.org
Price	:	₹ 750/- (For Module - I to Module VII, Including DVD)
ISBN	:	978-81-8441-335-9
Published by	:	The Publication Department on behalf of the Institute of Chartered Accountants of India, ICAI Bhawan, Post Box No. 7100, Indraprastha Marg, New Delhi-110 002.
Printed by	:	Finesse Graphics & Prints Pvt. Ltd. Tel.: 022-4036 4600 Fax : 022-2496 2297

Foreword

Information technology (IT) plays a vital role in supporting the activities of any organisation. The growth and change that has come about as a result of developments in technology have important implications. At the same time the increasing use of IT has also led to e-crimes like cyber warfare, hacking, data thefts, DDoS (Distributed Denial of Service) and other computer related frauds. Subsequently, there are various e-Governance, regulatory and compliance issues which are required to be looked into. These technological changes have put more focus on the role performed by Chartered Accountants, especially in the field of Information Systems Audit.

For Chartered Accountants there exist opportunities in Auditing and Assurance as well as consulting areas. Chartered Accountants with their expertise in data and indepth understanding of systems and process functions are uniquely suited for providing consulting in control implementation of IT enabled services as well as review of the same. IT by default rather than by design has become critically relevant for CA firms.

The Committee on Information Technology (CIT) of the Institute of Chartered Accountants of India (ICAI) was established to identify the emerging professional opportunities in the IT sector. It has also been conducting post qualification course on Information Systems Audit thus providing vast opportunities to Chartered Accountants. In view of the dynamism of the sector, a revised edition of the background material for the post qualification course on Information Systems Audit is being brought up by the CIT.

The background material contains various practical aspects, new technologies along with case studies related to Information Systems Audit, which will make this a great learning guide. I appreciate the efforts put in by CA. Rajkumar S. Adukia, Chairman, CA. Atul Kumar Gupta, Vice Chairman, other members and officials of CIT and faculty for bringing out the revised background material.

I hope that it will be a useful learning material and will assist the members in understanding the nuances of the Information Systems Audit. I wish our members great success in the field of Information Systems Audit.

Best Wishes

CA. Manoj Fadnis
President, ICAI

Preface

Information Technology has now emerged as the Business Driver of choice by Enterprises and Government Departments to better manage their operations and offer value added services to their clients/citizens. We now find increasing deployment of IT by enterprises and governments alike in geometric progression.

While the increasing deployment of IT has given immense benefits to enterprises and government departments, there have been increasing concerns on the efficiency and effectiveness of the massive investments made in IT, apart from the safety and security of Information Systems themselves and data integrity. As enterprises are increasingly getting dependent on IT Resources to manage their core business functionality, there are also concerns of Business Continuity.

It is a matter of immense pleasure for me that the Committee on Information Technology of the Institute has come out with the updated ISA Course 2.0 to equip members with unique body of knowledge and skill sets so that they become Information Systems Auditors (ISAs) who are technologically adept and are able to utilise and leverage technology to become more effective in their work and learn new ways that will add value to clients, customers and employers. This will also meet the increasing need of CAs with solid IT skills that can provide IT enabled services through consulting/assurance in the areas of designing, integrating and implementing IT Solutions to meet enterprise requirements.

The updated course material has taken into consideration the latest curriculum of similar professional courses and the recent/emerging developments in the field of Information Technology and IS Auditing and has been updated taking into consideration all the suggested changes and encompasses existing modules, contents and testing methodology.

The specific objectives of the updated ISA course 2.0 is: “To provide relevant practical knowledge and skills for planning and performing various types of assurance or consulting assignments in the areas of Governance, Risk management, Security, Controls and Compliance in the domain of Information Systems and in an Information Technology environment by using relevant standards, frameworks, guidelines and best practices.”

The updated ISA Course 2.0 has a blend of training and includes e-Learning, facilitated e-Learning, hands on training, project work in addition to class room lectures. This background material also includes a DVD which has e-Learning lectures, PPTs and useful checklists. The focus is to ensure that practical aspects are covered in all the modules as relevant. I am sure the updated ISA course 2.0 will be very beneficial to the members and enable them to offer IT assurance and advisory services.

I am sure that this updated background material on Information Systems Audit Course 2.0 would be of immense help to the members by enhancing efficiency not only in providing compliance, consulting and assurance services but also open out new professional avenues in the areas of IT Governance, assurance, security, control and assurance services.

Information Technology is a dynamic area and we have to keep updating our auditing methodologies and skill-sets in tune with emerging technologies. We hope this updated ISA 2.0 course is a step in this direction. We welcome your comments and suggestions.

CA. Rajkumar S. Adukia
Chairman
Committee on Information Technology

Table of Contents

CHAPTER 3: AUDIT OF BUSINESS CONTINUITY PLAN

INTRODUCTION TO BACKGROUND MATERIAL

Need for DISA 2.0 Course

Enterprises today in the rapidly changing digital world are inundated with new demands, stringent regulations and risk scenarios emerging daily, making it critical to effectively govern and manage information and related technologies. This has resulted in enterprise leaders being under constant pressure to deliver value to enterprise stakeholders by achieving business objectives. This has made it imperative for management to ensure effective use of information using IT. Senior management have to ensure that the investments and expenditure facilitate IT enabled change and provide business value. This can be achieved by ensuring that IT is deployed not only for supporting organisational goals but also to ensure compliance with internally directed and externally imposed regulations. This dynamic changing business environment impacted by IT provides both a challenge and opportunity for chartered accountants to be not only assurance providers but also providers of advisory services.

The updated ISA course 2.0 has been designed for CAs to provide IT enabled services with the required level of confidence so that management can have trust in IT and IT related services. The ISA course 2.0 builds on the existing core competencies of CAs and provides the right type of skills and toolsets in IT so that CAs can start exploring the immense potential of this innovative opportunity. A key component of this knowledge base is the use of globally accepted good practices and frameworks and developing a holistic approach in providing such services. The background material has been designed with practical perspective of using such global best practices.

Need for updation to DISA 2.0 course

The need for DISA course updation has been extensively discussed considering the objectives and utility of the course. It was decided to update the contents based on suggestions received considering the latest developments in the field of IT and IS Auditing. The updated course has revised modules with key areas of learning as practically relevant for CAs which will enable them to be more effective in their practice for regular compliance audits and also enable to provide IT assurance or consulting services. The updated syllabus has also considered the IT knowledge acquired by the latest batch of CA students who have studied IT in IPCC and Final and have also gone through practical IT trainings. A bridge DISA course is expected to be developed to help existing DISAs to update their knowledge and skills as per the latest course.

Objective of updated DISA Course

The objective of the updated DISA course 2.0 is to equip CAs with a unique body of knowledge and skill-sets so that they can become Information Systems Auditors (ISAs) who are technologically adept and are able to utilise and leverage technology to become more effective in their work and learn new ways and thus add value to their clients or employers. The updated DISA 2.0 course will also meet the increasing market need of CAs with solid IT skills who can provide consulting/assurance in the areas of designing, integrating and implementing IT Solutions to meet enterprise requirements. The updated syllabus of the DISA Course 2.0 has been prepared based on inputs from senior faculty and has undergone numerous reviews over a period of more than two years. The latest curriculum of similar professional courses and the recent/emerging developments in the field of IT and IS Auditing were also referred in updating the course.

Objective of updated DISA Course Material

The primary objective of the updated study material for DISA course is to ensure that DISAs are well versed with the latest IT concepts and practice in the areas of Governance of Enterprise IT, GRC, Assurance, risk, security and controls. The study material has a companion DVD which includes all the reading material and supplementary reference materials and checklists in soft copy. The DVD also includes the e-Learning content available as on date. All the contents in the DVD are presented and linked to aid in easy access of required material. Hence, the DVD and background material will be useful not only as a reading material for passing the DISA exam but also as a reference material for providing IT assurance and consulting services. The sample checklists given in the material can be customised based on scope, objectives of the assignment and considering the nature of business and the technology platform or the enterprise architecture.

Reading of this material is not a one-time exercise but has to be repeated and supplemented with other relevant material and research on the internet. As IT is a rapidly changing area, the material will be updated regularly. Although technology and the services provided using technology undergo rapid changes, the key concepts and requirements for risks, security and control will always remain whether it was the main-frame environment earlier or the mobile computing environment now. Hence, the need for audit and IS audit will always remain.

Use of structured approach

The updated syllabus has been developed by using process oriented structured approach based on the bloom taxonomy of learning and other global best practices. This covers the process/ guidelines to be adapted in development of updated study material.

Overall Objectives

The IT knowledge and skills acquired in the DISA course would enable DISAs to be more effective in using IT for auditing in a computerised environment in existing domains of compliance, consulting and assurance services. The overall objective of the DISA course 2.0 is: **"To provide relevant practical knowledge and skills for planning and performing various types of assurance or consulting assignments in the areas of Governance, Risk management, Security, Controls and Compliance in the domain of Information Systems and in an Information Technology environment by using relevant standards, frameworks, guidelines and best practices."**

Course Coverage

The DISA Course will provide basic understanding of how information technology is used and deployed. It facilitates understanding of how an IS Auditor is expected to analyse, review, evaluate and provide recommendations on identified control weaknesses in different areas of technology deployment. However, it is to be noted that the DISA course is not oriented towards teaching fundamentals of technology. The DISA course is conducted through a good blend of e-learning (online and facilitated), classroom training, hands-on training with practical case studies and project work to ensure practical application of knowledge. The DISA course combines technology, information assurance and information management expertise that enables a DISA to become trusted Information Technology advisor and provider of IS Assurance services. The DISA with

the unique blend of knowledge would serve as the "bridge" between business and technology leveraging the CA's strategic and general business skills. The class room training has been supplemented with hands on training. Aspiring DISAs need to remember that the class room training is not expected to be comprehensive but as aid to facilitate understanding. Considering the extensive coverage of the course, duration and the diverse level of participants, the faculty will not be able to cover the material indepth. **Please read the background materials of the specific modules prior to attending the classes to derive maximum benefit from the class room training.**

DISA Certification

DISA Certification through judicious blend of theoretical and practical training provides CAs with better understanding of IT deployment in enterprises which will enable them to be more effective not only in auditing in a computerised environment covering traditional areas of financial/ compliance audits but also in offering IT enabled services. The DISA exam is designed to assess and certify CAs for conducting IS Audit. After successfully completing the course, the DISA candidates are expected to have required knowledge and skills to perform various assurance and consulting assignments relating to Governance, Risk management, Security, Controls and Compliance in the domain of Information Systems, Information Technology and related areas.

DISA Course : Basic competency requirements

After successful completion of the course, the DISA candidates will have conceptual clarity and will demonstrate basic competency in the following key areas:

- Overall understanding of information system and technology: concepts and practice
- Risks of deployment of information system and technology
- Features and functionalities of security and controls of IT components and IT environment.
- Controls which could be implemented using the security features and functionalities so as to mitigate the risks in the relevant IT components and environments.
- Recommend IT risk management strategy as appropriate.
- Apply appropriate strategy, approach, methodology and techniques for auditing technology using relevant IS Audit standards, guidelines and procedures and perform IS Assurance and consulting assignments.

Modules of the DISA Course

The updated ISA certification is granted exclusively to CAs who demonstrate considerable expertise in domain areas of IT Governance, Security, Control and assurance through their knowledge, skills and experience The primary purpose of the ISA exam is to test whether the candidate has the requisite knowledge and skills to apply IS assurance principles and practices in the following modules:

No.	Name of Module	(%) Q's
1	Primer on Information Technology, IS Infrastructure and Emerging Technologies	20
2	Information Systems Assurance Services	13
3	Governance and Management of Enterprise Information Technology, Risk Management and Compliance Reviews	13
4	Protection of Information Systems Infrastructure and Information Assets	20
5	Systems Development: Acquisition, Maintenance and Implementation.	14
6	Business Applications Software Audit	13
7	Business Continuity Management	7

Learning Objectives

The DISA course is not expected to be an in-depth comprehensive coverage of different aspects of IT such as computer hardware, operating system, network, databases, application software, etc. but is focused on training on how to review IT controls and provide assurance on secure technology deployment.

The key learning objectives are:

1. Demonstrate understanding of functioning of key components of existing and emerging information technology and their practical deployment.
2. Provide IS assurance or IT Enabled services and perform effective audits in a computerised environment by using relevant standards, guidelines, frameworks and best practices.
3. Evaluate structures, policies, procedures, practices, accountability mechanisms and performance measures for ensuring Governance and management of Information Technology, risk management and compliance as per internal and external stakeholder requirements.
4. Provide assurance, consulting or compliance services to confirm that enterprise has appropriate security and controls to mitigate risks at different layers of technology as per risk management strategy.
5. Provide assurance or consulting services that the management practices relating to systems development: acquisition, maintenance and implementation are appropriate to meet enterprise strategy and requirements.

6. Provide assurance or consulting services to validate whether required controls have been designed, configured and implemented in the application software as per enterprise and regulatory requirements and provide recommendations for mitigating control weaknesses as required.
7. Provide assurance or consulting services to confirm whether the Business continuity management strategy, processes and practices meet enterprise requirements to ensure timely resumption of IT enabled business operations and minimise the business impact of a disaster.
8. Plan and perform IS assurance or consulting assignments by applying knowledge learnt by presenting project assignment relating to allotted case study to confirm understanding.

Skill Levels

The updated syllabus provides specific skills in each of the three categories of skill areas. The suggested skill levels ensure that the updated syllabus through all the modules has right blend of concepts and practice. The skill levels will be considered by the authors of study material and also in testing methodology through the eligibility tests and assessment test.

Weightage and category of skills

No.	Skills Category	Weightage (%)
1	Knowledge and Understanding	30 to 40
2	Application of the Body of Knowledge	55 to 60
3	Written communication	5 to 10

Summary of revised DISA Training

No.	Mode of Training	Weightage (%)
1	e-Learning Online (self)	12
2	e-Learning facilitated (lectures)	12
3	Classroom Training (lectures)	42
4	Hands-on Training (on laptop)	24
5	Project Work (self in groups)	10
	Total	**100**

Key highlights of DISA training

DISA Training includes e-Learning, hands on Training, project work in addition to classroom lectures.

- Candidates will have to successfully complete e-learning mode before joining classroom training.
- The training in classroom and hands-on training will follow the order in sequential order of the modules. This includes an inter-mix of classroom lectures and hands-on training. The hands-on training pre-supposes and builds on understanding of concepts of the classroom lectures.
- The training includes mandatory e-Learning of 12 hours for Module-1 and 6 hours for Module-2 and passing in the online test is mandatory and part of the eligibility score.
- Module-4 will have class room lectures of 2 days and hands on training of 2 days. Module-6 will have hands on training of 2 days. **Supplementary e-Learning Lectures covering Modules 4 and 6 are also included.** These will be added in due course and will be made available through DVD or online.
- **Hands on training for Module 4 and 6 will be conducted by the experienced faculty at same venue as class rooms with all participants performing exercises on their own laptops with pre-loaded software and sample/test data as specified in advance.**

DISA 2.0 Course Background Material

The DISA Course 2.0 Background Material is intended to assist in preparing for the DISA exam. The material is a one source of preparation for the exam, but should not be considered as the only source nor should it be viewed as a comprehensive collection of all the information that is required to pass the exam. Participants are encouraged to supplement their learning by using and researching the references provided in the material.

DISA 2.0 Course DVD

The Reading material for the DISA 2.0 course includes a DVD which is comprehensive collection of educational material for revised DISA Course 2.0. This DVD will aid self-learning and includes Background Material, Reference Material, e-Lectures, PowerPoint Presentations, Podcasts/MP3 Files and Self-Assessment Quiz (). This DVD is designed to be supplementary to the background material. It has to be used for self-learning and also as a training aide for the DISA Course 2.0 and DISA candidates are strongly advised to use this for studying for the ISA course.

Standard PPTs for each of the modules of the DISA 2.0 course have been prepared by the authors based on the background material. These are provided in the DVD only and are expected to serve as reference material during the class. Additional references materials and checklists of the course are only included in the DVD. The PPTs may be customised or updated by the faculty as required. Participants are encouraged to copy the DVD contents in their laptops and use this as reference in the classroom training.

Feedback and updates

We compliment you on choosing to join the DISA 2.0 Course and wish you a great learning experience. Please make best use of the material and the training. **Please note that the training is expected to supplement your reading of the material prior to attending the course.** Please participate actively in the training to make the best use of the training The material will be useful to you not only to aid you in preparing for exam but also for providing services in the area of Governance, Assurance and consulting.

Please note that the **background material has been contributed by practising professionals who have shared their expertise and reflects different writing styles of the authors.**

Please provide your feedback on areas of improvement of the course and the reading material in the specified format so that further improvements can be made. Please email your feedback or queries to: **isa@icai.in.** Please visit CIT portal http://cit.icai.org/ for the latest updates of the DISA course. We wish you a great learning experience and a rewarding career as an IS Auditor.

Committee of Information Technology, ICAI

The course material includes references to some specific companies, hardware or software. This reference is only for educational purposes and is not in any way endorsement of the company or products. All copyrights are acknowledged and belong to the rightful owners.

Module 7:

Business Continuity Management (7%)

Section: Overview

SECTION 1: CONTENTS
CHAPTER 1: BUSINESS CONTINUITY MANAGEMENT, BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY PLANNING

Learning objectives

The objective of this chapter is to provide knowledge about the key concepts of Business Continuity Management (BCM), Business Continuity Planning (BCP), Disaster Recovery Planning (DRP), Incident Responses, Contingency plan and disaster. It is important to understand these concepts as they form the base for the content that is explained in Chapters 2 and 3. DISA candidate is expected to have understanding of the key terms related concepts as this is critical for designing, implementing or reviewing business continuity. A good understanding and working knowledge in this area will help DISAs to provide assurance and consulting services in this area.

1.1 Introduction

Information is said to be the currency of the 21st century and it is considered the most valuable asset of an organisation. This is more so in case of organisations which use and are heavily dependent on Information Technology (IT). Organisations in this modern era run their business based on information which are processed using Information and Communication Technology (ICT). The ICT plays a central role in the operation of the business activities. For example, the stock market is virtually paperless. Banks and financial institutions have become online, where the customers rarely need to set foot in the branch premises. There is a heavy dependence on real time information from information technology assets for conducting business. Information is a critical factor for continued success of the business. This dependence on Information is more explicit in the most organisations which are now dependent on IT for performing their regular business operations. We can understand the criticality of IT by imagining impact of failure or non-availability of IT in case of following types of organisations:

- Bank using Core banking solution with a million accounts, credit cards, loans and customers.
- Companies using centralised ERP software having operations in multiple locations.
- An airline serving customers on flights daily using IT for all operations.
- Pharmacy system filling millions of prescriptions per year (some of the prescriptions are life-saving).
- Automobile factory producing manufacturing hundreds of vehicles daily using automated solution.
- Railways managing thousands of train routes and passengers through automated ticketing and reservation.

The above situations clearly demonstrate the heavy dependence on IT systems. IT can fail due to multiple factors. Hence, organisations should have appropriate contingency plans for resuming operations from disruption. The disruption of business operation can be due to unforeseen man-made or natural disaster and this may lead to loss of productivity, revenue and market share among many other impacts. Hence, organisations have to take necessary steps to ensure that the impact from such disasters is minimised and build resilience which ensures continuity of critical operation in the event of disruptions. Modern organisations cannot think of running their business operations without IT. IT is prone to increased risks which can lead to failure of IT thus impacting operations. Hence, it is becoming increasingly important for organisations to have a business contingency plan for their Information Systems.

The criticality of the plan can be determined based on the level of impact on critical business operations due to failure or non-availability of IT impacting service delivery. The failure of IT could be caused due to any or more of the following:

- Server or network failure
- Disk system failure
- Hacker break-in
- Denial of Service attack
- Extended power failure
- Snow storm, earthquake, tornado or fire
- Spyware, malevolent virus or worm
- Employee error or revenge
- Sabotage or theft

Organisations worldwide are more and more dependent on computers, in assisting and carrying out the decision making processes and in recording business transactions. An organisation is extremely dependent on several I.S. resources like computers, employees, Servers and communication links. If any of these resources are not available, the organisation will not be able to function at its full strength. The longer one or more of these resources are unavailable, the longer it takes the organisation to get back to its original state. Sometimes, organisations can never get back to its original state. As a result, it becomes important to have a tested plan for the disaster recovery, more importantly, in the information system area to ensure business continuity. The organisations that think ahead have a better chance of survival always.

1.2 Definitions of key terms

The concepts of Business Continuity Management are quite simple to understand. However, to understand and implement BCM or BCP as per needs of organisation requirements, it is know the key terms. Knowledge of definition of these terms will help not only in understanding the topics but also to provide assurance, consulting or implementation services in this area.

Business Continuity Planning: Business continuity planning is the process of developing prior arrangements and procedures that enable an organisation to respond to an event in such a manner that critical business functions can continue within planned level of disruption. The end result of the planning is called a Business Continuity Plan.

Business Continuity Plan: A documented collection of procedures and information that is developed compiled and maintained in readiness for use in an incident to enable an organisation to continue to deliver its critical products and services at an acceptable predefined level.

Business Continuity Management: A holistic management process that identifies potential threats to an organisation and the impacts to business operations that those threats – if realised – might cause, and which provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of its key stake holders, reputation, brand, and value-creating activities.

Business Impact Analysis: The process of analysing functions and the effect that a business disruption might have upon them.

Contingency Plan: A plan to deal with specific set of adverse circumstances.

Crisis: An abnormal situation which threatens the operations, staff, customers or reputation of the organisation.

Disaster: A physical event which interrupts business processes sufficiently to threaten the viability of the organisation.

Disaster Recovery Planning: A disaster recovery plan (DRP) is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster.

Emergency Management Team (EMT): This team comprising of executives at all levels including IT is vested with the responsibility of commanding the resources which are required to recover the enterprises operations.

Incident: An event that has the capacity to lead to loss of or a disruption to an organisation's operations, services, or functions – which, if not managed, can escalate into an emergency, crisis or disaster.

Incident Management Plan: A clearly defined and documented plan of action for use at the time of an incident, typically covering the key personnel, resources, services and actions needed to implement the incident management process.

Minimum Business Continuity Objective (MBCO): This refers to the minimum level of services and/or products that is acceptable to the organisation to achieve its business objectives during an incident, emergency or disaster. As per ISO 22301:2012, clause 3.28, MBCO is the minimum level of services and/or products that is acceptable to the organizations to achieve its business objectives during a disruption. MBCO is used to develop test plan for testing BCP.

Maximum Acceptable Outage (MAO): This is the time frame during which a recovery must become effective before an outage compromises the ability of an organisation to achieve its business objectives and/or survival. This refers to the maximum period of time that an organization can tolerate the disruption of a critical business function, before the achievement of objectives is adversely affected. MAO is also known as maximum tolerable outage (MTO), maximum downtime (MD). Maximum Tolerable Period Downtime (MTPD).

Resilience: The ability of an organisation to resist being affected by the incident.

Risk: The combination of the probability of an event and its consequence.

Vulnerability: The degree to which a person, asset, process, information, infrastructure or other resources are exposed to the actions or effects of a risk, event or other occurrence.

1.3 Key concepts of Disaster Recovery, Business Continuity Plan and Business Continuity Management

1.3.1 Contingency Plan (CP)

An organisation's ability to withstand losses caused by unexpected events depends on proper planning and execution of such plans. Without a workable plan, unexpected events can cause severe damage to information resources and may affect the business continuity. Contingency planning is an overall process of preparing for unexpected events. Its main goal is to restore normal modes of operation with minimal cost and minimal disruption to normal business activities after unexpected event. It should ideally ensure continuous information systems availability despite unexpected events.

Components of contingency planning

1. Business impact analysis (BIA)

BIA includes tasks like Threat Attack identification and prioritization, Business unit analysis, Attack scenario development, Potential damage assessment, etc. The steps involved in impact analysis are risk evaluation, defining critical functions in the organisation, identifying critical facilities required for providing recovery of the critical functions and their interdependencies and finally setting priorities for all critical business applications which need to be recovered within defined timelines. The details of this concept have been highlighted in 2.4.

2. Incident response plan (IR plan)

IR Plan includes tasks like incident planning, incident detection, incident reaction, incident recovery etc. Incident Response plan gives an entity a set of procedures and guidelines that is needed by an entity to handle an incident. The details of this concept have been highlighted in 2.8.

3. Business continuity plan (BCP)

BC Plan includes tasks like establishing continuity strategies, planning for continuity of critical operations, continuity management etc. Business Continuity Plan is a plan that contains the steps that would be taken by an entity to resume its business functions during its period of disruption. These plans are executed in parallel with the disaster recovery plans depending on the impact of the disaster. Business Continuity Plans on a whole is about reestablishing existing business processes and functions, communications with the business contacts and resuming business processes at the primary business location.

4. Disaster recovery plan (DRP)

DR Plan includes tasks like plan for disaster recovery, crisis management, recovery operations etc. Disaster Recovery Plan is the set of plans which are to be executed initially at the moment of crisis. These plans include measures to control the disaster, mitigate them and to initiate the recovery of the resources that is needed for the continuity of business. These plans are targeted to initiate/recover the resources that have been affected by a disaster. These are the first plans that would be executed at the time of disaster.

There are three basic strategies that encompass a disaster recovery plan: preventive measures,

detective measures, and corrective measures. Preventive measures will try to prevent a disaster from occurring. These measures seek to identify and reduce risks. They are designed to mitigate or prevent an event from turning into a disaster. These measures may include keeping data backed up and off site, using surge protectors, installing generators and conducting routine inspections. Detective measures are taken to discover the presence of any unwanted events within the IT infrastructure. Their aim is to uncover new potential threats. They may detect or uncover unwanted events. These measures include installing fire alarms, using up-to-date antivirus software, holding employee training sessions, and installing server and network monitoring software. Corrective measures are aimed to restore a system after a disaster or otherwise unwanted event takes place. These measures focus on fixing or restoring the systems after a disaster and may include keeping critical documents in the DRP or securing proper insurance policies.

1.3.2 Business ContinuityPlan vs. Disaster Recovery Plan

The primary objective of Business Continuity Plan is to ensure that mission critical functions and operations are recovered and made operational in an acceptable time frame. A BCP aims to sustain critical business process during an unplanned interruption period and a DRP is to re-establish the primary site into operation with respect to all business processes of the organisation facing the disaster.

1.3.3 Business Continuity Management

BCM is a holistic process that identifies potential threats and the impacts on normal business operations should those threats actualise. BCM provides a framework to develop and build the organisation's resilience with the capability for an effective response, therefore ensuring that critical objectives are met, safeguarding key stakeholder’s interests and the organisation's reputation, brand and value creating activities. The purpose of BCM is to minimise the operational, financial, legal, reputational and other material consequences arising from a disruption due to an undesired event (Basel Committee on Banking Supervision, 2005), minimising losses and restoring normal, regular operations in the shortest, possible time. Coupled with security measures to protect the organisation's assets, BCM requires plans and strategies that should cater for and allow responses, contingency plans and procedures to recover as quickly as possible. BCM looks at an entirety of the businesses of the entity as a whole. It is a continuous process whereby risks which are inherent to the business are closely monitored and mitigated.

1.4 Objectives of BCM and BCP

1.4.1 Objectives of Business Continuity Plan

The primary objective of a Business Continuity Plan (BCP) is to enable an organisation to continue to operate through an extended loss of any of its business premises or functions.

The key objectives of BCP are:

- Manage the risks which could lead to disastrous events.
- Reduce the time taken to recover when an incident occurs and

- Minimise the risks involved in the recovery process
- Reduce the costs involved in reviving the business from the incident

1.4.2 Objectives of Business Continuity Management (BCM)

The objective of BCM is to counteract interruptions to business activities and to protect critical business processes from the impact of major failures or disasters. The detailed objectives of BCM are:

- Reduce likelihood of a disruption occurring that affects the business through a risk management process
- Enhance organisation's ability to recover following a disruption to normal operating conditions
- Minimise the impact of that disruption, should it occur
- Protect staff and their welfare and ensure staff knows their roles and responsibilities
- Tackle potential failures within organisation's I.S. Environment
- Protect the business
- Preserve and maintain relationships with customers
- Mitigate negative publicity
- Safeguard organisation's market share and/or competitive advantage
- Protect organisation's profits or revenue and avoid financial losses
- Prevent or reduce damage to the organisation's reputation and image

Need for BCM at business Level

The need for BCM arises because of the following present day requirements of business

- Need to provide access to potentially millions of new customers
- Need to ensure security, privacy and confidentiality
- Need to integrate business processes onto web
- Need to integrate business partners into key business processes
- Increased pressure on delivering quality customer service 24x7
- Emerging pervasive computer devices

Business and organisations of today depend heavily on Information and Communication Technology (ICT) to conduct business. The ICT plays a central role in the operation of the business activities. For example, the stock market is virtually paperless. Banks and financial institutions have become online, where the customers rarely need to set foot in the branch premises. This dependence on the systems means that all organisations should have contingency plans for resuming operations from disruption. The disruption of business operation can be due to unforeseen manmade or natural disaster that may result into revenue loss, productivity loss and loss of market share among many other impacts. Thus organisations have to take necessary steps to ensure continuity of operation in the event of disruptions. Business continuity is the activity performed by an organisation to ensure that critical business functions will be available

to customers, suppliers, regulators, and other entities that must have access to those functions. These activities include many daily chores such as project management, system backups, change control, and help desk. Business continuity is not something implemented at the time of a disaster; Business Continuity refers to those activities performed daily to maintain service, consistency, and recoverability.

Need for BCM at various levels of IT Environment.

Disaster Recovery is an essential phase to critical IT Resources. IT Infrastructure generally includes Servers, Workstations, Network and Communication, Operating system software, business applications software, essential utility software, Data Centres, Support Desks, IT Personnel, Disks, Tapes etc. In this technologically driven world, IT Infrastructure has essentially become an integral part of an entity's anatomy. Mail Servers and communication lines like Internet, Phone and Fax are also essentially the important components of the Infrastructure. It is therefore critical to get these components up and running for a successful recovery of the business. Therefore when critical industries like Banks, Insurance Companies, Stock Exchanges, Airline Companies, Railways, Multinational Companies, Government Agencies rely on IT Infrastructure for its daily operations, it is crucial to maintain BCM for such organisations. Software like the Core Banking Systems, SWIFT Financial Messaging Services, Airline Communication Services like AMADEUS, Stock Market Trading Applications, ERP Systems, e-commerce sites and many more are critical where no downtime is tolerated. These applications are used to conduct transactions worldwide and are run only on extensive IT Resources. BCM therefore is a much needed requirement for a quick recovery from a crisis to ensure survival of the business.

1.5 What is a disaster?

BCM or BCP is all about planning in advance to meet future unforeseen events which may impact or disrupt business operations. Disasters are the major source of disruptions. As distinguished from an event which causes disruption for a short period of time and addressed through incident management plan, disaster are of various types and can have varying and serious impact. This section will provide an overview of various types of disasters.

A disaster can be defined as an unplanned interruption of normal business process. It can be said as a disruption of business operations that stops an organisation from providing critical services caused by the absence of critical resources. An occurrence of disaster cannot always be foreseen; hence we need to be prepared for all the types of disasters that can arise, handle them effectively in the shortest time.

Vulnerabilities are also a major cause or source of disasters. Vulnerabilities are weaknesses associated with an organisation's assets. These weaknesses may be exploited by a threat causing unwanted incidents that may result in loss, damage or harm to those assets. Vulnerability in itself does not cause harm; it is merely a condition or set of conditions that may allow a threat to affect an asset. Vulnerability is weakness of an asset or group of assets, which can be exploited by a threat. As part of risk assessment exercise, it is important to understand the various vulnerabilities and threats and coupled with probability, organisation can assess the impact. This will be evaluated in business impact analysis and mitigated appropriately by implementing appropriate counter measures. In contemporary academia, disasters are seen as the consequence of inappropriately managed risk. These risks are the product of a combination of both hazard/s and vulnerability. Hazards that strike in areas with low vulnerability will never become disasters, as is the case in uninhabited regions.

1.5.1 Types of disasters

A disaster can be natural or man-made (or technological) hazard resulting in an event of substantial extent causing significant physical damage or destruction, loss of life, or drastic change to the environment. A disaster can be defined as any tragic event stemming from events such as earthquakes, floods, catastrophic accidents, fires, or explosions. It can cause damage to life and property and destroy the economic, social and cultural life of people. For a clearer understanding of the concept of disasters, disasters can be classified into two major categories as:

1. Natural disasters
2. Man-made disasters

1. Natural disasters

Natural Disasters are those which are a result of natural environment factors. A natural disaster has its impact on the business's that is present in a geographical area where the natural disaster has struck. Natural disasters are caused by natural events and include fire, earthquake, tsunami, typhoon, floods, tornado, lightning, blizzards, freezing temperatures, heavy snowfall, pandemic, severe hailstorms, volcano etc.

2. Man-made disasters

Man-made disasters are artificial disasters which arise due to the actions of human beings. Artificial disasters has its impact on a business entity specific to which it has occurred. Artificial disasters arising due to human beings Include Terrorist Attack, Bomb Threat, Chemical Spills, Civil Disturbance, Electrical Failure, Fire, HVAC Failure, Water Leaks, Water Stoppage, Strikes, Hacker attacks, Viruses, Human Error, Loss of Telecommunications, Data Centre outrage, lost data, Corrupted data, Loss of Network services, Power failure, Prolonged equipment outrage, UPS loss, generator loss and anything that diminishes or destroys normal data processing capabilities.

1.5.2 Phases of disaster

It is important to envisage what is the impact when a disaster strikes and decide in advance the action to be taken for various types of disaster scenarios. A typical disaster will consist of some or all of the following phases:

1. Crisis phase
2. Emergency response phase
3. Recovery phase
4. Restoration phase

1. Crisis phase

The Crisis Phase is under the overall responsibility of the Incident Control Team (ICT). It comprises the first few hours after a disruptive event starts or the threat of such an event is first identified; and is caused by, for example:

- Ongoing physical damage to premises which may be life threatening, such as a fire; or
- Restricted access to premises, such as a police cordon after a bomb incident. During the crisis phase, the fire and other emergency evacuation procedures (including bomb threat and valuable object removal procedures) will apply; and the emergency services should be summoned as appropriate.

2. Emergency response phase

The Emergency Response Phase may last from a few minutes to a few hours after the disaster. It will start near the end of, or after, the crisis Phase if there has been one, or when a potentially threatening situation is identified. During the Emergency Response Phase, the Business Continuity Team (BCT) will assess the situation; and decide if and when to activate the BCP.

3. Recovery phase

The Recovery Phase may last from a few days to several months after a disaster and ends when normal operations can restart in the affected premises or replacement premises, if appropriate. During the recovery phase, essential operations will be restarted (this could be at temporary premises) by one or more recovery teams using the BCP; and the essential operations will continue in their recovery format until normal conditions are resumed.

4. Restoration phase

This phase restores conditions to normal. It will start with a damage assessment, usually within a day or so of the disaster, when the cause for evacuation or stopping of operations has ended, normal working will be restarted. During the restoration phase, any damage to the premises and facilities will be repaired.

1.5.3 Examples of disaster

Some examples of disasters and the phases that may impact disaster phases of a business continuity plan are:

Examples of Disaster	Phases
Serious fire during working Hours	All phases in full
Serious fire outside during working hours	All the phases, however, no staff and public evacuation
Very minor fire during working hours	Crisis Phase only, staff and public evacuation but perhaps no removal of valuable objects, Fire Service Summoned to deal with the fire
Gas mail leak outside during working hours, repaired after some hours	Only emergency response phase is appropriate

1.5.4 Impact of disaster

The impact of a disaster can vary and could result in:

- Total destruction of the premises and its contents. For example as a result of a terrorist attack;
- Partial damage, preventing use of the premises. For example through flooding; or
- No actual physical damage to the premises but restricted access for a limited period, such as enforced evacuation due to the discovery nearby of an unexploded bomb.

The impact of a disaster may result in one or more of the following:

ii. **Loss of human life:** The extent of loss depends on the type and severity of the disaster. Protection of human life is of utmost importance and, the overriding principle behind continuity plans.

iii. **Loss of productivity:** When a system failure occurs, employees may be handicapped in performing their functions. This could result in productivity loss for the organisation.

iv. **Loss of Revenue:** For many organisations like banks, airlines, railways, stock brokers, effect of even a relatively short breakdown may lead to huge revenue losses.

v. **Loss of Market share:** In a competitive market, inability to provide services in time may cause loss of market share. For example, a prolonged non-availability of services from services providers, such as Telecom Company or Internet Service Providers, will cause customers to change to different service providers.

vi. **Loss of goodwill and customer services:** In case of a prolonged or frequent service disruption, customers may lose confidence resulting in loss of faith and goodwill.

vii. **Litigation:** Laws, regulations, contractual obligation in form of service level agreement govern the business operations. Failure in such compliance may lead the company to legal litigations and lawsuits.

When considering the impact of a disaster, it should be remembered that it will never happen at a convenient time; and is always unpredictable. There is no way of knowing:

- When it will happen;
- What form it will take;
- How much damage it will cause; or
- How big the impact will be.

However, it is important to envisage various types of scenarios to ensure that the coverage is as comprehensive as feasible covering various types of events with varying impact. Understanding disaster and their impact is the key to successful business impact analysis which will result to preparation of an effective business continuity plan.

1.6 Summary

This chapter has provided an overview of the key concepts relating to management of BCP, DRP and Incident Responses. Together, these are to be implemented as part of Business Continuity Management. The ultimate objective of a BCM is to recover from a crisis as fast as possible and at the lowest possible cost. Business Continuity is applicable to organisations of all sizes and types of business. Business Continuity is most crucial to organisations which use IT Resources for their critical business functions. We have also understood that the need for BCP arises due to a disruptive event which could be result in a disaster. Disaster is an event that causes interruption to the ongoing business functions which is either natural or man-made. The phases of a disaster crisis phase, emergency response phase, recovery phase and restoration phase have also been discussed.

1.7 Questions

1. An organisation's disaster recovery plan should address early recovery of:
   - A. All information systems processes.
   - B. All financial processing applications.
   - C. Only those applications designated by the IS Manager.
   - D. Processing in priority order, as defined by business management.
2. Which of the following is MOST important to have in a disaster recovery plan?
   - A. Backup of compiled object programmes
   - B. Reciprocal processing agreement
   - C. Phone contact list
   - D. Supply of special forms
3. Which of the following BEST describes difference between a DRP and a BCP? The DRP:
   - A. Works for natural disasters whereas BCP works for unplanned operating incidents such as technical failures.
   - B. Works for business process recovery and information systems whereas BCP works only for information systems.
   - C. Defines all needed actions to restore to normal operation after an un planned incident whereas BCP only deals with critical operations needed to continue working after an un planned incident.
   - D. Is the awareness process for employees whereas BCP contains procedures to recover the operation.
4. The MOST significant level of BCP programme development effort is generally required during the:
   - A. Early stages of planning.
   - B. Evaluation stage.
   - C. Maintenance stage.
   - D. Testing Stage.

5. Disaster recovery planning for a company's computer system usually focuses on:
   A. Operations turnover procedures.
   B. Strategic long-range planning.
   C. The probability that a disaster will occur.
   D. Alternative procedures to process transactions.
6. An unplanned interruption of normal business process is?
   A. Risk
   B. Vulnerability
   C. Disaster
   D. Resilience
7. Which of the following strategy does not encompass disaster recovery plan?
   A. Preventive
   B. Detective
   C. Corrective
   D. Administrative
8. Which of the following is not a fundamental of BCP?
   A. Manage the risks which could lead to disastrous events
   B. Minimise the risks involved in the recovery process
   C. Reduce the costs involved in reviving the business from the incident
   D. Mitigate negative publicity
9. Which phase starts with a damage assessment?
   A. Crisis Phase
   B. Emergency Response Phase
   C. Recovery Phase
   D. Restoration Phase
10. Which of the following is of utmost important during an impact of disaster?
   A. Loss of Productivity
   B. Loss of Revenue
   C. Loss of Human Life
   D. Loss of Goodwill & Market Share

1.8 Answers and Explanations

1. D. Business management should know what systems are critical and when they need to process well in advance of a disaster. It is their responsibility to develop and maintain the plan. Adequate time will not be available for this determination once the disaster occurs. IS and the information processing facility are service organisations that exist for the purpose of assisting the general user management in successfully performing their jobs.
2. A. Of the choices, a backup of compiled object programmes is the most important in a successful recovery. A reciprocal processing agreement is not as important, because alternative equipment can be found after a disaster occurs. A phone contact list may aid in the immediate aftermath, as would an accessible supply of special forms, but neither is as important as having access to required programmes.
3. C. The difference pertains to the scope of each plan. A disaster recovery plan recovers all operations, whereas a business continuity plan retrieves business continuity (minimum requirements to provide services to the customers or clients). Choices A, B and D are incorrect because the type of plan (recovery or continuity) is independent from the sort of disaster or process and it includes both awareness campaigns and procedures.
4. A. A company in the early stages of business continuity planning (BCP) will incur the most significant level of program development effort, which will level out as the BCP program moves into maintenance, testing and evaluation stages. It is during the planning stage that an IS Auditor will play an important role in obtaining senior management's commitment to resources and assignment of BCP responsibilities.
5. D. It is important that disaster recovery identify alternative processes that can be put in place while the system is not available.
6. C. Disasteris event which interrupts business processes sufficiently to threaten the viability of the organisation. Risk is a combination of the probability of an event and its consequence. Vulnerability is the degree to which a person, asset, process, information, infrastructure or other resources are exposed to the actions or effects of a risk, event or other occurrence. Resilience is the ability of an organisation to resist being affected by the incident.
7. D. There are three basic strategies that encompass a disaster recovery plan: preventive measures, detective measures, and corrective measures. Preventive measures will try to prevent a disaster from occurring. These measures seek to identify and reduce risks. Detective measures are taken to discover the presence of any unwanted events within the IT infrastructure. Their aim is to uncover new potential threats. Corrective measures are aimed to restore a system after a disaster or otherwise unwanted event takes place.
8. D. Mitigate negative publicity is an objective of Business Continuity Management is to rest all are the fundamental aim of BCP.
9. D. Restoration phase will start with a damage assessment, usually within a day or so of the disaster, when the cause for evacuation or stopping of operations has ended, normal working will be restarted. During the Restoration Phase, any damage to the premises and facilities will be repaired.
10. C. Protection of human life is of utmost importance and, the overriding principle behind continuity plans. Rest all are to be considered later.

CHAPTER 2: STRATEGIES FOR DEVELOPMENT OF BUSINESS CONTINUITY PLAN

Learning Objectives

This chapter forms the core of Business Continuity Management (BCM). The objective of this chapter is to provide understanding on how to design a Business Continuity Plan (BCP). The key steps of BCP such as Business Impact Analysis, performing risk assessment and designing tests for the BCP are explained. BCP requires planning in advance and planning requires extensive documentation and communication so that implementation happens as per plan. Specific aspects of BCP which need to be documented are explained with sample contents, steps and procedures. These cover BCP manual, backup and recovery strategies, recovery and alternate sites, other strategies and types of insurance requirements. Critical events such as how and when to invoke a disaster recovery plan and the specific tasks and responsibilities are explained. This chapter it explains what management has to do in case of BCP. A thorough knowledge of these topics will help DISAs will help them to perform a BCP Audit or providing consulting services on any/all aspects of BCP. BCP audit is explained in next chapter.

2.1 Introduction

An organisation's ability to wheather losses caused by unexpected events depends on proper planning and execution of such plans. Without a workable plan, unexpected events can cause severe damage to information resources and assets. Normally businesses that don't have a disaster plan go out of business after a major loss like a fire, a break-in, or a storm. A formal policy provides the authority and guidance necessary to develop an effective Business Continuity plan. The Business Impact Analysis helps to identify and prioritise critical IT systems and components. It also helps to identify the control measures to be in place to reduce the effects of system disruptions, to increase system availability and to reduce contingency life cycle costs. Developing planned recovery strategies ensures that critical information systems are recovered quickly and effectively following a disruption. Business impact analysis helps organisations in choosing the right recovery strategies. The BCP should contain detailed guidance and procedures to be followed till the restoration of damaged system. Testing the plan identifies planning gaps, whereas recovery plan helps in training the personnel for plan activation; both activities improve plan effectiveness and overall organisation preparedness. BCP should be a living document that is updated regularly as per defined policy.

2.2 Pre-requisites in developing a Business Continuity Plan

Regulatory and stakeholder requirements mandate the responsibility on the management of all organisations to ensure that all critical business processes are identified; risks associated with the processes are determined, adequate measures of redundancy are built in and around the processes, to minimise the effect of loss, should there be a disaster. Understanding of regulatory requirements as applicable through various legislations applicable in the international scenario like Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II), Sarbanes-Oxley, HSPD-12, BASEL II, Gramm-Leach-Bliley are essential in developing BCP. Most of the global

best practices and frameworks such as COBIT, ISO 27001 and ISO 22301 emphasise the critical need of BCP for organisations.

A BCP cannot be considered as a project which is completed within specified time. BCP has to be a continuous process and has to be an integral part of the day-to-day business processes. BCP to be effective has to be tested and updated regularly and at least once a year, if not more frequently. Critical business functions may keep changing and hence a plan that does not keep pace with the changes in the organisation is not of any use. Therefore, one may have a working BCP on a given day, but the BCP has to be a continuous affair to ensure success.

The primary objectives of a BCP are to guide an organisation in the event of a disaster and to effectively re-establish critical business operations within the shortest possible period of time with minimal loss of data. The pre-requisite in developing a BCP includes planning for all phases and making it part of business process by assigning responsibility to specific business process owners. The goals of planning the project are to assess current and anticipated vulnerabilities, define the requirements of the business and IT, design and implement risk mitigation procedures and provide the organisation with a BCP that will enable it to react quickly and efficiently in event of a disaster.

The objectives of planning the project is to gain an understanding of the existing and planned future IT environment of the organisation, define the scope of the project, develop the project schedule, and identify risks to the project. In addition, a project sponsor/champion and steering committee should be established. The project sponsor or champion should be a member of senior management team with required authority to push the project to completion. The steering committee should be responsible for guiding the project team. The committee should have members from both functional and IT departments. Further, a project manager and/or a BCP co-ordinator should be appointed to lead, monitor completion and maintain the project. In implementing a BCP project, the key tasks are:

- Define the scope of the planning effort
- Develop a plan framework
- Assemble a project team and conduct awareness sessions

Just as every organisation is unique, so too is the business continuity planning project. As such each plan should be tailored to the individual organisation, what works for one organisation may not necessarily work for another. The major phases in developing a BCP are:

1. Business Impact Analysis,
2. Risk Assessment,
3. Actual Planning and design of the BCP and the BCP Manual i.e., development of BCP
4. Testing of the BCP,
5. Training and awareness to the employees and
6. Maintenance of the BCP.

2.2.1 Phase 1: Business Impact Analysis

The business impact analysis (BIA) establishes the needs of an organisation for recoverability and sets the requirements for its recovery strategy and ultimately its recovery plan. The BIA also can be used to achieve other objectives within an organisation. Firstly, a BIA can be used to prioritise

the recovery sequence of data, infrastructure, etc. Secondly, a BIA can define the minimum operating requirements a business needs to recover operations following a disruption. These things include Information Technology resources, human capital, etc. Thirdly, a BIA presents the value proposition for implementing the appropriate level of recoverability. If it can be demonstrated that a disruption of certain number of minutes, hours or days will have effect on a company's reputation, finances and operations, then simple prudence calls for an organisational response, in the form of both recovery plan and recovery infrastructure, i.e., a plan to prevent disruption or to mitigate its impact. The broad outline of a strategy should be apparent in BIA results. A BIA presents requirements for disaster recovery plans. The narrative outline for a BIA strategy could be as follows:

1. We rely on the 10 data centres to do business.
2. In case of disruption, we would only have 7 data centres available to us.
3. We cannot obtain 3 data centres in a reasonable timeframe.
4. Therefore we need to arrange for alternate data centers in advance of a disruption.

Item number four is the basis of the BIA strategy. Once it is made self-evident that an alternate data centre is a requirement, there are other steps an organisation needs to take to properly prepare for a disaster, i.e., size the DR facility, decide on internal vs. outsourced solutions, determine how to get data from one site to another, and so on. The important message of a BIA is that the status quo will not suffice and that some investment is essential. Further analysis will balance the competing imperatives of risk reduction, capital expenditure, service availability, operating expense and P&L impact. If stakeholders do not see the big picture, they surely will not accept the details.

Recovery Strategy Budget Planning

		Vendor Costs	Hardware Costs	Software Costs	Travel/ Shipping Costs	Labour/ Contract or cost	Testing Costs	Supply Costs
Alternate Site	Cold site							
	Warm Site							
	Hot Site							
	Mobile Site							
	Mirrored Site							
Offsite Storage	Commercial							
	Internal							
Equipment Replacement	SLAs							
	New							
	Existing repairs & use							

BIA is the first phase in Contingency planning process. It provides data about systems and threats faced. It also provides detailed scenarios/effects of attacks. Contingency Planning team conducts Business Impact Analysis in the following stages:

– Threat attack identification and prioritisation
– Business unit analysis
– Attack success scenario development
– Potential damage assessment
– Subordinate plan classification
• The following Issues are to be considered for Business Impact Analysis
– Different business processes
– Critical information resources related to critical business processes
– Critical recovery time period before significant losses are incurred Systems risk ranking

2.2.2 Phase 2: Risk assessment and methodology of risk assessment

Risk Assessment seeks to identify which business processes and related resources are critical to the business, what threats or exposures exist to cause an unplanned interruption of business processes, and what impact accrues due to an interruption. There are various analytical procedures that are used to determine the risks, threats, and exposures faced by an organisation. These are known by various names, such as Business Impact Analysis (BIA), Application Impact Analysis, Threat and Exposure Analysis, Risk Impact Analysis and so on. While many authors and practitioners maintain subtle differences between these terms, this discussion subsumes all these activities under Risk Assessment.

Risk is an exposure to unwanted loss. In terms of Business Continuity, it is the risk of an incident happening which may result in unwanted loss of an asset or delay in operations.

Risk Assessment is the systematic identification of all risks, their investigation and grading relevant to each other and to the department, so that the management can be given a clear and full understanding of the risks it faces.

Risk Assessment is an important phase in the development of a Business Continuity Plan (BCP). The objective of Risk Assessment are to:

• identify the risks that organisation faces
• Identify the threat that the organisation would face
• Identify the source of threat
• identify essential operations that must be restarted as quickly as possible after a disaster has taken place;
• identify cost-effective measures that could be introduced to prevent risks or lessen their impact and
• provide an input for risk management.

All disaster events may not be anticipated or considered. For example, very few organisations considered Tsunami as a major risk in South Asia, before it actually struck.

Risk Assessment & Recovery

The objectives of risk assessment include:

1. **Criticality prioritisation:** Identifying business functions or processes and their associated resource requirements. Prioritising business processes according to their time-sensitivity and criticality.

2. **Estimating the critical recovery time period:** (also called “Recovery Time Objectives" or "Maximum Tolerable Downtime") of the business process. The critical recovery time period is the maximum amount of time allowed for the recovery of the business function. This is the amount of downtime of the business process that the business can tolerate and still remain viable. If this time is exceeded, then severe damage to the organisation will result. From the IT point of view, recovery usually means restoring support for the processing and communication functions that are considered to be critical to the business and then restoring support for other non-critical/ancillary systems. From the business perspective, recovery means being able to execute the business functions that are at the key to the survival of the business and then being able to execute the non-critical/ancillary functions. Another key factor to consider when defining recovery is the timeframe. Recovery of the function and the system is evaluated considering several time based factors such as:

    i. **Recovery Time Objective (RTO):** RTO is the measure of the user’s tolerance to downtime. It indicates the earliest point in time at which the business operations must resume after disaster. For example: Critical monitoring system must have very low RTO or zero RTO. RTO may be measured in minutes or less.

    ii. **Service Delivery Objective (SDO):** Service Delivery Objective (SDO) is the level of services to be reached during the alternate process mode until the normal situation is restored. This is directly related to the business needs.

    iii. **Recovery Point Objective (RPO):** RPO is a measure of how much data loss due to a node failure is acceptable to the business. A large RPO means that the business can tolerate a great deal of lost data. Depending on the environment, the loss of data could have a significant impact. A rule of thumb is that the lower the RPO, higher the overall cost of maintaining the environment for recovery. An RPO of 5 minutes can lose data up to 5 minutes of data, whereas 0 RPO will have no loss of data. Like RTO/SDO, RPO may vary with services and system. However, it is important to understand the dependencies between the systems and to be taken into consideration while determining the critical systems. These objectives are not closely related – they may both be almost zero, they may both be large, or one may be small but the other large. Once a company decides what RPO and RTO are applicable to an application, the method for backup and recovery of that application becomes much more evident.

Examples of need of various systems in different organisations and scenarios are illustrated here:

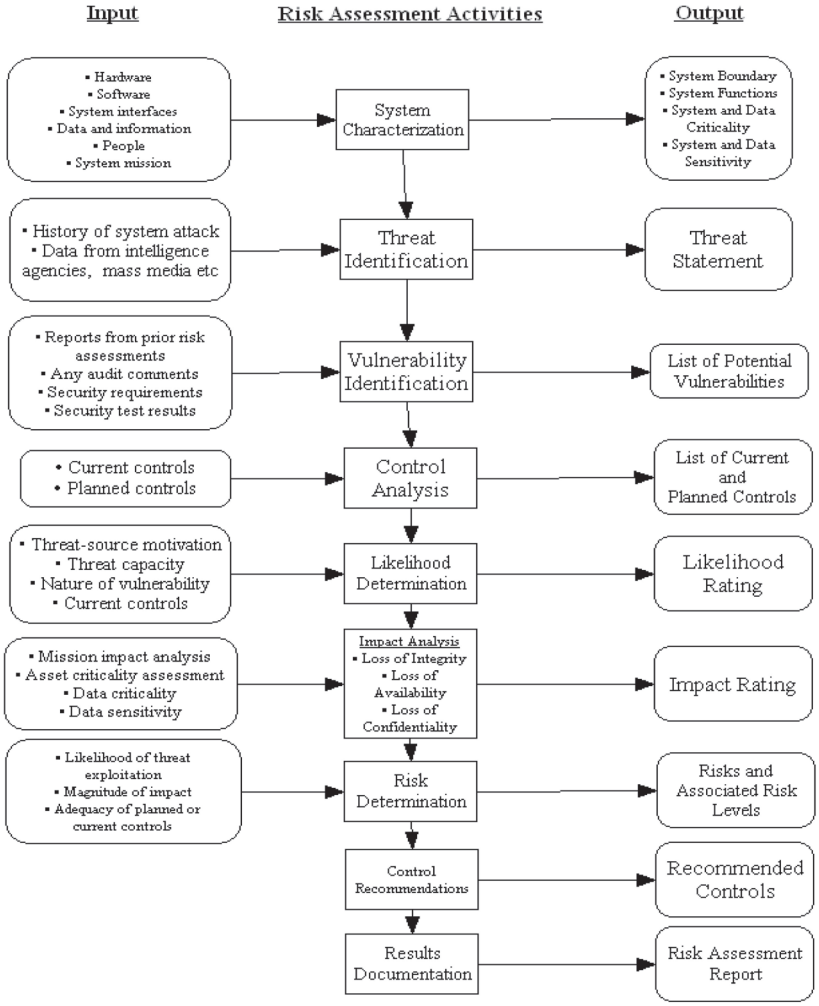
    i. A stock exchange trading system must be restored very quickly and cannot afford to lose any data. Since the price of the next trade depends upon the previous trade, the loss of a trade will make all subsequent transactions wrong. In this case, the RTO may be measured as a few minutes or less, but the RPO must be zero.

    ii. A critical monitoring system such as those used by power grids, nuclear facilities, or hospitals for monitoring patients must have a very small RTO, but the RPO may be large. In these systems, monitoring must be as continuous as possible;

but the data collected becomes stale very quickly. Thus, if data is lost during an outage (large RPO), this perhaps impacts historical trends; but no critical functions are lost. However, an outage must end as quickly as possible so that critical monitoring can continue. Therefore, a very small RTO is required.

iii. A Web-based online ordering system must have an RPO close to zero (the company does not wish to lose any sales or, even worse, acknowledge a sale to a customer and then not deliver the product). However, if shipping and billing are delayed by even a day, there is often no serious consequence, thus relaxing the RTO for this part of the application.

iv. A bank's ATM system is even less critical. If an ATM is down, the customer, although aggravated, will find another one. If an ATM transaction is lost, a customer's account may be inaccurate until the next day when the ATM logs are used to verify and adjust customer accounts. Thus, neither RPO nor RTO need to be small.



Maximum Tolerable outages: Maximum tolerable outage is the maximum time the organisation can support processing in alternate mode. After this point, different problems may arise, especially if the alternate SDO is lower than usual SDO and the information pending to be up-to-date can become unmanageable.

Interruption window: Interruption window is the time the organisation can wait from the point of failure to the critical services/applications restoration. After this time, the progressive losses caused by the interruption are unaffordable.

Threats and its type

The threats, exposure, probability of happening and the loss are documented as part of the Risk Assessment. An analysis of all the business processes that are supported by IT will be carried out to identify the systems / processes that are critical / core to very survival of the business and also to determine the length of time that such processes can survive without IT by not incurring heavy loss. The information should be gathered through standard survey tools or questionnaires and should be documented in a clear and understandable format to be presented to the management. A threat is anything with a potential for adverse effect on an asset, for example fire, unauthorized access to premises. Threats should be assessed to determine:

- How vulnerable the organisation's assets are to the threats
- What preventative measures could be taken to lessen the impact of the threats

The different types of threat an organisation's assets may be at a risk from are as follows:

- Natural
  - Fire
  - Flood
  - Storm
  - Lightning
  - Power Failure
- Deliberate/Intentional
  - Bomb
  - Sabotage
  - Theft
  - Strike
- Accidental
  - Outrage
  - Errors
  - Disclosure

Organisations should also consider threats arising from various issues as:

- Unauthorised access to:
  - Premises
  - Equipment

- Papers and other resources
- Computer systems, from outside and inside the premises

- Location of the premises
  - Road, Rail and air traffic
  - Industrial processes
  - Visible targets for terrorism
  - Entrances and Exits
- Shared Premises
  - Should agree who is responsible for what
  - Are legally required to co-operate and co-ordinate during an emergency

Risk assessment has to be a coordinated activity with participation from personnel departments, vendors and interested stakeholders. A sample checklist which can be used for risk assessment is given below:

Sample checklist for Risk Assessment

Areas for Investigation Status	(Y/N) / Comment
Existence of fire and other emergency evacuation procedures	
Existence of bomb threat procedures	
Reliance on telephone, fax, IT equipment	
List of reliable contractors for emergency repairs	
Dependency on specific goods and services	
Dependency on specific equipment	
Computer data backed up and stored off site	
Compliance with legislation on public health, health and safety, fire precautions	
Compliance with listed building constraints	
Leakages, burst pipes, internal flooding water, oil, gas	
Power isolation devices on electrical systems	

Risk Assessment Methods

If the Risk Management is to be effective, a systematic approach to Risk Assessment should be taken. This means that Risk Assessment should be conducted formally, rather than casually. The following methods will enable a systematic and reliable risk assessment to be carried out:

1. Risk Ranking
2. Value ranges
3. Formulae for comparing risks
4. Computer software if suitable

1. Risk Ranking

The ability of a company to cope with interruption of a business process determines the TOLERANCE of the business process. This tolerance depends on the length of the disruption and may also be linked to the time of the day or month the interruption occurs. In practice, tolerance is usually expressed as a monetary amount – the cost to the company if business process is interrupted for a given unit of time. This cost of interruption is inversely related to the tolerance. The various business processes may be classified on their critical recovery time period.

i. **Critical:** These are functions that cannot be done manually under any circumstances. Unless a company located identical capabilities to replace the damaged capabilities, these functions cannot be performed. These functions have zero or very low tolerance to interruption and consequently, the cost of interruption is high.

ii. **Vital:** These functions can be performed manually but only for a brief period of time. There is relatively higher tolerance to interruption as compared to critical functions and consequently somewhat lower cost of interruption. The function classified as vital can withstand a brief suspension of operations but cannot withstand an extended period of downtime.

iii. **Sensitive:** These processes can be carried out by manual means for an extended period, though with some difficulty. They may require additional staff to perform and when restored, may require considerable amount of time to restore the data to current or usable form.

iv. **Non-Critical:** These processes have a high tolerance to interruption and can be interrupted for an extended period of time with little or no adverse consequences. Very little time is required to restore the data to a current or usable form.

2. Value ranges

To assist in comparison, a range of values should be set for each of the following:

- Asset cost
- Likelihood of threat happening
- Vulnerability; and
- Assessment of the risk

The following ranges can be used

- A scale of one to five; or
- Very Low, Low, Moderate, High and Very High

A scale of one to five will produce a more accurate Risk Assessment than a scale of one to three. Ranges greater than five are usually unnecessary and should only be used if a particularly accurate Risk Assessment is required, or a greater distinction between different risks needs to be made.

3. Formulae for comparing risks

To produce more precise results from a Risk Assessment, a formula can be used in conjunction with the value ranges in mentioned above to compare and priorities risks. For example:

$$\text{Risk} = \frac{\text{Asset Cost} + \text{Likelihood} + \text{Vulnerability}}{3}$$

Divide the sum of asset cost, likelihood and vulnerability by three to find the average value. For convenience, the resulting score can then be translated into words to describe the risk, such as:

- 1 -Very Low;
- 2 - Low;
- 3 - Moderate;
- 4 - High;
- 5 -Very High.

Example: The risk of flooding to a premise has been assessed and the following values awarded:

- Asset cost = 5 (the property is highly valued);
- Likelihood = 3 (flood is considered to be a moderate threat because the property is located in the midland); and
- Vulnerability = 2 (because the property is constructed well above the ground level/Sea level).

Using the formula given above, the score for this particular risk is:

$$\frac{5 + 3 + 2}{3} = 3.3$$

This translates into words as `Moderate' risk.

4. Formula Method for Comparing Risks

The risk is calculated from the analysis of threats, vulnerabilities and impacts on key assets. Where the risk is unacceptable, steps should be taken to reduce it by applying measures to reduce the impact, threat or vulnerability to an acceptable level. The risk will be determined by an algorithm, based on ascribing values to the risk that is based on the values already ascribed to the threat, vulnerability and impact. There is no universally appropriate formula for this process, but it approximates to: Risk = Threat x Vulnerability x Impact

Thus, a threat, which had a high impact, might still be rated highly although its occurrence would be relatively rare. Conversely, a frequent threat (especially where the organisation was vulnerable) could be rated highly even though its impact was only minor. The example above and the above formulae used are simple and should be adequate for uncomplicated Risk Assessments.

2.2.3 Phase 3: Development of BCP

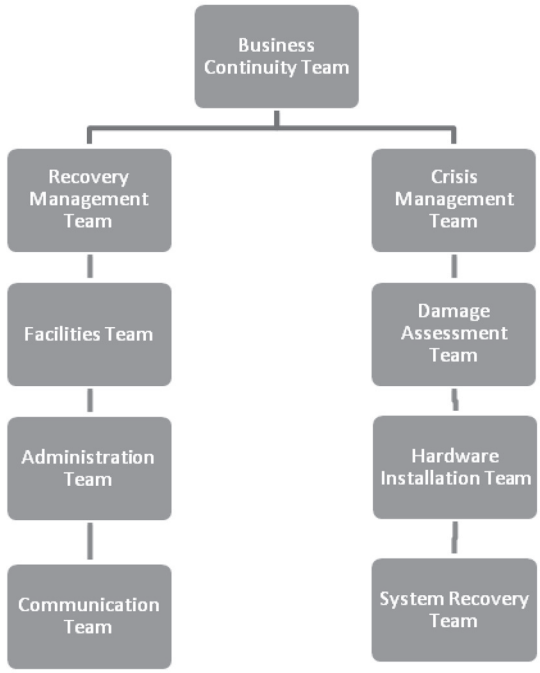
Based on the inputs received from BIA, a detailed plan is then developed. It should ideally address all issues involved in a disruption to business processes and recovery from a disaster. The plan should be documented and written in simple language, so that everyone in the organisation and related to the organisation including, if necessary, third-party vendors etc. understands it. It should be a part of the plan to develop some important teams with clear cut roles and responsibilities. Some of such important teams are:

Business Continuity Team

i) **Recovery Management Team:** The recovery management team will oversee and manage any recovery exercise. Leaders of all other teams should form part of the management team, to ensure that complete and up-to-date information is presented at all status meetings. The business continuity planning co-ordinator or administrator will be part of team. Any decisions on revising the recovery process or reacting to changed circumstances will be made by this team. The manager of this team will also report to senior corporate management who are not intimately involved in the process. Even where multiple sites are covered by the plan, the membership of this team will be relatively constant. Only the leaders from the site specific recovery team will vary.

ii) **Crisis Management/Public Relations Team:** Dealing with external agencies or interest groups is an inevitable part of any post-disaster activity. The work performed by this team may extend beyond the provision of detail on what has happened, and what is being done to keep the business in operation. For example, this team may also have to handle:

- Notification of death or injury to next of kin
- Dealing with the media
- liaison with government or regulatory bodies and
- Handling public concerns if the disaster has health or environmental implications



Business Continuity Team

To be effective, this team must have all of the necessary information at their disposal and include appropriate senior corporate officials who are comfortable in dealing with the media and relaxed in front of cameras. Mishandling public relations can severely damage an organisation's reputation and cause more harm than the disaster itself.

Dealing with the media is a skill which must be developed, and there are consulting firms which specialise in this service. In addition to being comfortable in the handling of the media, this team must have a predefined plan for issuing statements, an agreed location for making those statements and an understanding of the level of information to be issued. Experience has shown that saying nothing or "no comment" can be more costly to the organisation than providing full and open disclosure. If the media cannot get the information from official sources, it is very good at finding other, not necessarily reliable, information from other sources.

The crisis management team or public relations team must be thoroughly prepared to handle the media and all other external communications. Appropriate spokespersons should be identified and trained. The functionalities of teams under the control of Recovery Management team and Crisis management team are elaborated below:

i) **Hardware Installation Team:** In today's business environment, it is likely that a recovery operation will require the installation of some computer equipment. This may include the ordering and installation of a replacement data centre, the installation of the specific terminals and printers required by the impacted business unit, or even the replacement of microcomputers.

ii) **System recovery Team:** Once the hardware team has completed its job, the system recovery team will be responsible for installing the necessary software, recovering data backup and ensuring that the recovered systems are capable of supporting the critical business functions.

iii) **Communications Team:** The communications team is responsible for handling the re-routing or re-connection of the essential voice and data communications. Because of the specialised nature of the communications functions, many large and decentralised organisations still maintain a centralised communications group.

iv) **Facilities Team:** Ensuring a smooth transition to temporary premises, and the refurbishment or replacement of the primary premises is among the responsibilities of the facilities team. This team may also be responsible for equipping the premises with furniture, office supplies and coffee making facilities.

v) **Administration Team:** The various recovery teams will each require administrative support. This will be one of the functions of the administration team. Administration team staff may also be responsible for such matters as staff travel arrangements, catering, petty cash control, telephone services, mail services, and some personnel functions.

vi) **Damage Assessment Team:** Damage assessment will be one of the first activities performed after a disaster occurs. Depending on the nature of the operations at the site impacted, the performance of such an assessment may require a number of different skill sets.

vii) Other teams which may be established include:

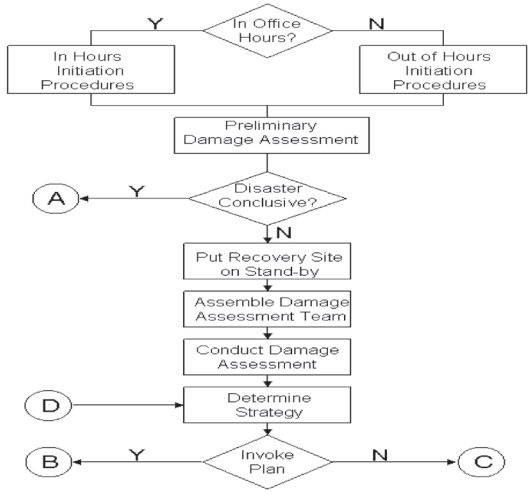
- **Application recovery team** – To recover specific critical application systems
- **Logistics team** – To assist in team co-ordination, if staffs are located at geographically separate sites for recovery purpose. This team can handle the distribution of mail and reports, movement of input documents and media, etc.
- **Staff co-ordination team** – Responsible for keeping staff informed of the situation and providing interim financial assistance to families, where required. Employees

can be great representatives in times of stress, but can also cause problems if they feel mistreated

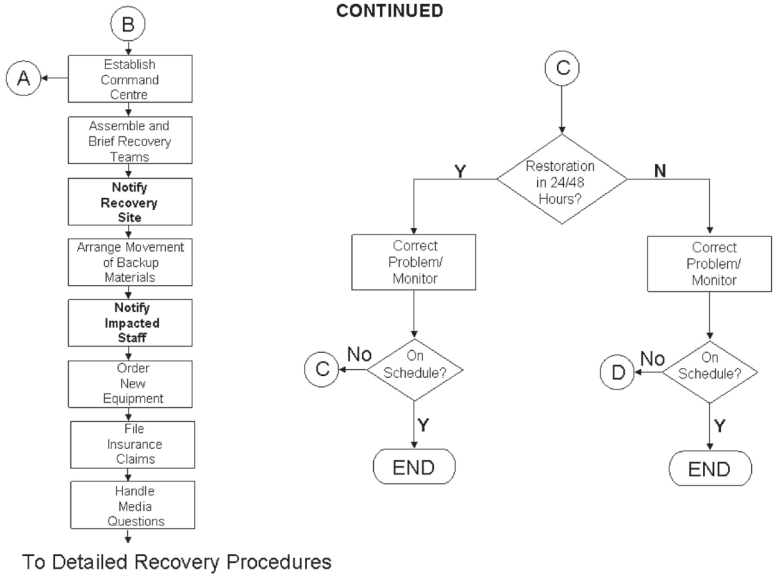
- **An insurance team** – Responsible for turning the damage assessment information into timely insurance claims
- **User liaison team** – Responsible for communications between a data centre recovery site and the remote users of that site

Once the teams have been established and their responsibilities agreed upon, details of the teams should be entered into the plan. This does not require step by step procedures, but an overview of each team's responsibilities and understanding of the interaction required between the teams.

DISASTER NOTIFICATION AND PLAN ACTIVATION



DISASTER NOTIFICATION AND PLAN ACTIVATION CONTINUED



Business Continuity Plan

The Business Continuity Plan should minimum encompass the following:

- **Initiation procedures:** Notification procedures will ensure that the organisation's appropriate officials are contacted on a timely basis when a disaster event occurs. These procedures will include contact details all of key personnel and vendors.
- **Preliminary damage assessment:** Once management has been notified of the problem, a preliminary damage assessment should be performed. This need not be a detailed assessment, but will provide an initial indication as to whether the plan needs to be activated.
- **Put recovery site on standby:** Where the BCP involves the use of a commercial recovery centre, that site should be put on notice. Most vendors favour being put on notice and appreciate an advance warning.
- **Assemble damage assessment team:** If the preliminary assessment is not conclusive, the full damage assessment team can be assembled. If all staff is on site when disaster strikes, this should be a relatively easy task. However if the incident occurs after office hours it will be necessary to call staff at home to notify all team members of the problem.
- **Conduct damage assessment:** The damage assessment process should be conducted as soon as possible following disaster notification. The assessment of the extent of the damage, possible duration of service disruption, and job processing status will directly impact the subsequent course of recovery action. The assessment process should consider the impact on:
  - The facilities
  - Power and other utilities
  - The environment and
  - Essential equipment

- **Determining strategy :** The identification of the most appropriate strategy will typically require a decision by the recovery management team, based on the damage assessment report. Once an appropriate strategy has been identified, the adoption of that solution must be approved by the senior management.
- **Establish emergency command centre :** While it may not be necessary to establish command centre for the damage assessment team alone, once the decision has been made to invoke the plan it will be necessary to activate that location. All members of the teams responsible for recovery of the management should assemble at an identified Emergency Command Centre. This center must be established at a predefined location within easy access of the primary site, but sufficiently far removed that it will not be affected by a disaster event. It is from this site that recovery operations will be directed.
- **Assemble and brief recovery teams :** This effect the notification of all team members to report to the command centre. This should include:
  - ✓ Giving details of who is calling
  - ✓ Providing a brief synopsis of disaster status

- ✓ Instruction to call all staff or alternates on the list of the person being called
- ✓ Instruction on where to report, when and with what materials and
- ✓ A record of all calls made should be retained.

- **Notify recovery site:** The recovery to be used including any commercial sites, should be notified of the decision to use the facility and requested to prepare the site in accordance with the contract.
- **Arrange movement of backup materials:** Once the decision is made to move to the recovery site, all of the necessary materials should be recovered from off-site storage and shipped to that location. The shipment of any required special forms from backup supplies should also be coordinated at this time.
- **Notify impacted staff:** Once the recovery operations are under way, the staff that will be impacted but will not be required for recovery activities should also be notified. It is preferable that they receive notification from the organisation rather than from the media.
- **File Insurance claims:** It may not be possible to file the claims immediately, as further damage assessment may still be required However as soon as the necessary information is available, the claims should be prepared.
- **Detail procedures for recovery:** A step by step instructions for recovering systems at recovery site should be written down. Some of instructions are:
  - Assemble and check site
  - Check off site materials and install equipment
  - Test operating system
  - Recover applications
  - Test applications
  - Hire temporary staffs
  - Update to disaster (if the recovery site is not shadowing all data processed at the primary site, data entry up to the state of disaster will be entered again at the recovery site)
  - Process backlog
  - Configure networks and test network
  - Establish external links
  - Redirect mail
  - Redirect communications
  - Correct problem / monitor
  - Establish controls
- **Primary site procedures:** While the detailed recovery procedures are concentrated on alternate facilities to restore the critical business operations, the primary site should be built up again. Steps remain to be taken in that location following the damage assessment and the decision to invoke the plan.

- **Return to normal operations:** Once the primary site is refurbished or a new primary site available, it is necessary to relocate to that site.
- **Post recovery reviews:** Once the return to normal operations has been completed and approved, the normal job schedules and operating instructions should be reintroduced. In addition, a review of the recovery operations should be performed to identify any areas in which the plan can be improved. This post mortem should be performed as soon as possible to ensure that concerns and problems experienced are still clear in staffs' minds.

The next step would involve the documentation of the plan which means creation of the BCP Manual. A BCP Manual houses all the relevant steps of the plan that is needed to be followed during a crisis. A BCP manual contains the Disaster Recovery Plans, Business Continuity Plan and the contingency plans. The elements of a BCP Manual are discussed in 2.10.

2.2.4 Phase 4: Testing of BCP and DRP

Testing the Disaster Recovery Plan

The Disaster Recovery Co-ordinator is responsible for testing of the disaster recovery plan at least annually to ensure the viability of the plan. However, special tests are to be given consideration whenever there has been a major revision to the plan or significant changes in the software, hardware or data communications have occurred. The objectives of testing the disaster recovery plan are:

1. Simulate the conditions of an ACTUAL Business Recovery situation
2. Determine the feasibility of the recovery process
3. Identify deficiencies in the existing procedures
4. Test the completeness of the business recovery information stored at the Offsite Storage Location.
5. Train members of the disaster recovery teams

The initial test of the plan will be in the form of a structured walk-through and should occur within two months of the disaster recovery plan's acceptance. Subsequent tests should be to the extent determined by the Business continuity co-ordinator that are cost effective and meet the benefits and objectives desired.

Sample Recovery Test agenda

Sample Recovery Test Agenda	
1.	What is the purpose of the test?
2.	What are the test objectives?
3.	How will the successful achievement of these objectives be measured?
4.	At the conclusion of the test, collect test measurements from all participants
5.	Evaluate the test results. Determine if the test was successful or not
6.	Determine the implications of the test results. Does success for this test imply success in all recovery scenarios?
7.	Update the plan based on results of the test

BCP Testing

The effectiveness of BCP has to be maintained through regular testing. The five types of tests of BCP are:

1. Checklist test
2. Structured walk through test
3. Simulation test
4. Parallel test
5. Full interruption test

1. **Checklist test:** In this type of test, copies of the plan are distributed to each business unit's management. The plan is then reviewed to ensure that the plan addresses all procedures and critical areas of the organisation. In reality, this is considered as a preliminary step to real test and is not a satisfactory test in itself.
2. **Structured walk through test:** In this type of test, business unit management representatives meet to walk through the plan. The goal is to ensure that the plan accurately reflects the organisation's ability to recover successfully, at least on paper. Each step of the plan is walked through in the meeting and marked as performed. Major faults with the plan should be apparent during the walk through.
3. **Simulation test:** In this type of test, all of the operational and support personnel who are expected to perform during an actual emergency meet in a mock practice session. The objective is to test the ability and preparedness of the personnel to respond to a simulated disaster. The simulation may go to the point of relocating to the alternate backup site or enacting recovery procedures, but does not perform any actual recovery process or alternate processing.
4. **Parallel test:** A Parallel test is a full test of the recovery plan, utilising all personnel. The difference between this and the full interruption test is that the primary production processing of the business does not stop, the test processing runs in parallel to the real processing. The goal of this type of test is to ensure that critical systems will actually run at the alternate processing backup site. Systems are relocated to the alternate site, parallel processing backup site, and the results of the transactions and other elements are compared. This is the most common type of disaster recovery plan testing.
5. **Full interruption test:** During a full interruption test, a disaster is replicated event the point of ceasing normal production operations. The plan is implemented as if it were a real disaster, to the point of involving emergency services. This is a very severe test, as it can cause a disaster on its own. It is the absolute best way to test a disaster recovery plan, however, because the plan either works or doesn't.

Documentation of results: During every phase of the test, a detailed documentation of observations, problems and resolutions should be maintained. This documentation can be of great assistance during an actual disaster. They are also helpful in improving and maintaining the plan as they reveal the strengths and weaknesses of the plan. No test is ever a failure because, however badly it may seem to have gone lessons can still be learnt from it. However, it should be remembered that if a test is not planned properly, it could actually create a disaster. Live tests especially could create disaster if not planned properly because they use real people and real

resources in real conditions, probably during normal working hours. Live tests should only be considered after the BCP has been tested in full and all Recovery Team members fully trained. The worst way to test a Plan is to turn off the power suddenly, for example, and tell people to exercise their Recovery Plans, the interruption and delay to normal work could well become a disaster in itself.

Results Analysis : The results of each test should be recorded to identify:

I. What happened

II. What was tested successfully; and

III. What needs to be changed?

If a test indicates that the BCP needs to be changed, the change should be made and the test repeated until all aspects are completed satisfactorily. When all the components have been tested satisfactorily, the whole BCP is ready for testing. It should not be assumed that because the components work individually there is no need to test the whole BCP. Putting it all together may reveal problems which did not show up in lower level testing. When preparing for testing, the participants should be given all the information and instruction they need.

2.2.5 Phase 5: Training and Awareness

Training the Team

The Disaster Recovery Co-ordinator is responsible for the co-ordination of training relating to the disaster recovery plan. The purpose of this training is two-fold:

1. To train recovery team participants who are required to execute plan segments in the event of a disaster.
2. To train the management and key employees in disaster prevention and awareness and the need for DRP.

The training of organisation's user management in disaster recovery planning is crucial. A DRP must have the continued support from organisation's user management to ensure future effective participation in plan testing and updating. It is not solely the responsibility of the Disaster Recovery Co-ordinator to initiate updates to the disaster recovery plan. User management must be aware of the basic recovery strategy; how the plan provides for rapid recovery of their information technology systems support structure. It is the responsibility of each recovery team participant to fully read and comprehend the entire plan, with specific emphasis on their role and responsibilities as part of the recovery team. On going training of the recovery team participants will continue through plan tests and review of the plan contents and updates provided by the Disaster Recovery Co-ordinator.

From the start of the BCP development project, positive action to create awareness of the BCP during the development, testing and training phases should be taken by holding briefings for all staff at an early stage of BCP development to explain the reasons for the BCP and its benefits to everyone and how it will be developed; The organisation should take care that all new staff are briefed about the BCP as a part of their induction to the organisation. It should be remembered that every test also trains the participants. If the full Recovery Teams are not used in each test, the participants should be rotated so that they all gain an adequate experience. At the end of the testing phase, further training and experience requirements should be identified. The Recovery Team leaders should be consulted for their opinions as they should have the best understanding of the present abilities of their team members.

Training methods

The training methods to be used may include:

1. Walk through session
2. Scenario workshop; or
3. Live test simulation

1. Walkthrough Session

For a walkthrough session, the participants sit round a table, each with a copy of the BCP (or appropriate part of the BCP), and `walk' through it by reading and discussing each part in sequence. Walkthrough sessions should be conducted at a quiet place without interruption because the objective is to identify any weaknesses, errors and omissions by allowing participants' thoughts to flow freely as they go through the plan. The only limit on discussion is that the whole part must be read to the end. All components of the BCP should first be tested using this method as it is highly likely to identify changes needed. One good walkthrough per component is usually sufficient if the suggested changes are then reviewed and agreed by a few of the esters for one Recovery Team. Links with other Teams should be noted and raised during their walkthroughs.

2. Scenario Workshop

This is similar to a walkthrough except that a scenario is devised before the workshop, and the key members of recovery teams are involved, although it is preferable to include all teams.

Scenarios should be designed:

1. Around the actual conditions of the premises and its operations
2. To introduce any possible disaster in a realistic way
3. To give a good testing of the plan
4. To include developments that would usually occur during a disaster, for example, changes in safety conditions delaying return to the premises.

Participants should sit round a table at a quiet place without interruption with their copies of the BCP (or appropriate part of the BCP), but instead of reading through the whole BCP, they should role-play their participation in the scenario. As they do so, they should say aloud what they are thinking and doing. The objective is to identify errors, omissions and weaknesses, and to establish whether the plan performs as intended. For this method to be effective, participants must:

1. Accepts the scenario at face value
2. Become fully involved in the role play; and
3. Voice all their thoughts and imagined actions. Brief interruptions to a participant’s spoken thoughts and actions are permitted if other participants have constructive comments or questions.

As the scenario progresses the lead participant(s) may change as appropriate to the timescale of the plan, particularly if the whole BCP is being tested rather than one Recovery Team's Plan. Participants need to be aware of this possibility so that it happens smoothly in the right places.

3. Simulation of a Live Test

The simulation of a live test:

1. Is held outside normal working hours so that resources can be used without affecting normal operations;
2. Involves the use of the planned and contracted contingencies if this is practical;
3. Requires relocation of some staff to another site if appropriate; and
4. Has to be as near to real life as possible so that all aspects of the BCP, including contingencies, are tested.

Because it is a test, some shortcuts may be taken, such as sending only a token number of people to the contingency site, or doing only token amounts of work to prove that the operation has been successfully recovered. However, even if shortcuts are used it must still be possible at the end of the test to conclude that all aspects of the BCP are effective. A simulation of a live test, perhaps more than the other methods, needs to be carefully planned to:

1. Ensures that the testing is thorough
2. Avoid confusion when things go wrong; an
3. Prevent any disruption to the real operations

2.2.6 Phase 6: Maintenance of BCP and DRP

Maintenance of the plans is critical to the success of an actual recovery. The plans must reflect changes to the environments that are supported by the plans. It is critical that existing change management processes are revised to take recovery plan maintenance into account. In areas, where change management does not exist, change management procedures will be recommended and implemented. Many recovery software products take this requirement into account. BCM testing, maintenance and audit testify the organisation BCM to prove the extent to which its strategies and plans are complete, current and accurate; and Identifies opportunities for improvement. Agreements may also need to reflect the changes. If additional equipment is needed, it must be maintained and periodically replaced when it is no longer dependable or no longer fits the organisation's architecture. The BCM maintenance process demonstrates the documented evidence of the proactive management and governance of the organisation's business continuity programme; the key people who are to implement the BCM strategy and plans are trained and competent.

The monitoring and control of the BCM risks faced by the organisation; and the evidence that material changes to the organisation's structure, products and services, activities, purpose, staff and objectives have been incorporated into the organisation's business continuity and incident management plans. Similarly, the maintenance tasks undertaken in development of BCP are to:

- Determine the ownership and responsibility for maintaining the various BCP strategies within the organisation
- Identify the BCP maintenance triggers to ensure that any organisational, operational, and structural changes are communicated to the personnel who are accountable for ensuring that the plan remains up-to-date
- Determine the maintenance regime to ensure the plan remains up-to-date
- Determine the maintenance processes to update the plan; and
- Implement version control procedures to ensure that the plan is maintained up-to-date

Role of IS Auditor in testing of BCP

- Ensure that a suitable mechanism exists to update the plan.
- The IS auditor should review the result of the Business Continuity Plan test. The IS auditor should check to see that the results of the test were along anticipated lines. If not, discrepancies between expected outcomes and actual outcomes should be analyzed to find shortcomings in the plan. The IS auditor should examine whether the weaknesses and shortcomings that have been identified during testing have been rectified at a later date.

2.3 Incident Handling and Management

2.3.1 Incident Response

Incident response (IR) is the set of procedures that commence when an incident is detected. For each attack scenario end case, IR team creates procedures to be deployed during, after, and before the incident. IR planning (IRP) follows these general stages:

– Form IR planning team

– Develop IR policy

– Organise security incident response team

– Develop IR plan

– Develop IR procedures

Incident Response Planning for: Before the Incident

IRP for before the incident consists of both preventative measures to manage risks associated with particular attack and activities to ensure IR team preparedness. Process includes:

– Training the Incident Response Team

– Testing the IR plan

– Selecting and maintaining tools used by the IRT

– Training users of the systems and procedures controlled by the organisation

Incident Response Planning for: Response during the Incident

Most important phase of the IR plan is the reaction to the incident. Each viable attack scenario end case is examined and discussed by the IR team:

✓ Trigger (circumstances that cause IR team activation and IR plan initiation) are to be defined

✓ What must be done to react to the particular situation are to be elaborated

✓ How to stop the incident if it is ongoing is also to be addressed along with the way by which the Elimination of problem source can be achieved

Incident Response Planning for: After the Incident

During this phase, the goal is to return each system to its previous state. IR plan must describe stages necessary to recover from most likely events of the incident. It should also detail other

events, like protection from follow-on incidents, forensic analysis, and the after-action review. After-action review (AAR) should explain about the detailed examination of events that occurred from first detection to final recovery.

2.3.2 Incident Classification

Incident classification is the process of evaluating organisational events, determining which events are incident candidates, and then determining whether it is an actual incident or a non event. IR design team creates process used to make this judgment; IR team actually classifies events. Incident candidates can be detected and tracked via reports from end users, intrusion detection systems, virus management software, and systems administrators.

Three broad categories of incident indicators are: possible, probable and definite.

Four types of possible actual incidents are: Presence of unfamiliar files, presence or execution of unknown programmes or processes, unusual consumption of computing resources and unusual system crashes.

Four probable indicators of actual incidents are: Activities at unexpected times, presence of new accounts, reported attacks and notification from IDS.

Five events of definite indicators of an incident are: Use of dormant accounts, modified or missing logs, presence of hacker tools, notifications by partner or peer and notification by hacker.

Five events which indicate that an incident is underway are: Loss of availability, loss of integrity, loss of confidentiality, violation of policy and violation of law.

2.3.3 Norms and procedure for declaring an Incident as a Disaster

Collection of data under IRP

Routine collection/analysis of data is required to properly detect/declare incidents. Logs should be enabled, stored off site and in a hardened location. Managing logs include the preparation of the system for amount of data generated, Rotation of the logs on schedule, encryption of logs, the archival and disposal of logs.

Reactions to incidents

How and when to activate IR plans determined by IR strategy organisation chooses to pursue? In formulating incident response strategy, many factors influence an organisation's decision. IR plan designed to stop incident, mitigate effects, and provide data that facilitates recovery. Two general categories of strategic approach for an organisation as it responds to an incident are 1. Protect and forget and 2. Apprehend and prosecute.

Incident Notifications

As soon as IR team determines an incident is in progress, appropriate people must be notified in the correct order. Alert roster is the document containing contact information for individuals to be notified during an incident. There are two ways to activate alert roster namely sequentially and hierarchically. Alert message should contain the scripted description of incident containing enough information for each responder to know what to do on alert process.

Documenting an Incident

Documenting the incident should begin immediately after incident is confirmed and notification process is underway. It should record who, what, when, where, why, and how of each action taken while incident is occurring. The purpose is to make the documentation to serve as case study to determine whether right and effective actions were taken. It helps to prove that the organisation did everything possible to prevent spread of the incident. It can also be used as simulation in future training sessions on future versions of IR plan.

Incident containment strategies

One of the most critical components of IR is stopping incident or containing its scope/impact. Affected areas must be identified. Incident containment strategies focus on two tasks namely stopping the incident and recovering control of the affected systems. IR team can attempt to stop incident and try to recover control by means of several strategies.

Recovering from incident

Once incident is contained and system control regained, incident recovery can begin with the Incident damage assessment (i.e.) immediate determination of the scope of the breach of confidentiality, integrity, and availability of information and information assets. Steps to be taken in the recovery process include Identifying and resolving vulnerabilities, restoration of data, restoration of services and processes, and restoration of confidence across the organisation.

After action review

Ongoing IR plan maintenance includes procedures to conduct after-action reviews, plan review and maintenance; train staffs involved in incident response, and rehearse process that maintains readiness for all aspects of the incident plan. IR team must conduct after-action review that is the detailed examination of events during incident. After Action Review serves as review tool, historical record, case training tool, closure

Incident response plan review and maintenance

At periodic intervals, an assigned member of management should review the IR plan. When shortcomings are noted, plan should be reviewed and revised to remediate deficiency. Organisation must undertake training programmes to ensure a sufficient pool of qualified staff are available to execute the plan when activated. Ongoing and systematic approach to planning requires plans be rehearsed until responders are prepared to perform as expected.

2.4 Invoking a DR Phase/BCP Phase

2.4.1 Operating Teams of contingency planning

Contingency Planning team: This team collects data about information systems and threats, conducts business impact analysis, and creates contingency plans for incident response, disaster recovery, business continuity. The primary role of this team is to conduct research on data that could lead to a crisis and develop actions that would effectively handle these threats.

Incident Response team: This team manages/executes IR plan by detecting, evaluating, responding to incidents. This team is the first team to arrive during the outbreak of an incident. Incident Response Team evaluates the incident, takes the first action to stop the incident. If unsuccessful, then summons the Disaster Recovery Team.

Disaster Recovery team: This team manages/executes DR plan by detecting, evaluating, responding to disasters; re-establishes primary site operations. This team plays its role in reducing the impact of the disaster and executes the steps that are defined in the DR Plan to recover and protect resources that are being impacted by the disaster and to mitigate the disaster itself. If the impact of the crisis is very high, then the Business Continuity Team steps in parallel to the DR Team and

Business Continuity Team: This team manages/executes BC plan by establishing off-site operations to ensure Business Continuity. Business Continuity Team initiates those responses to the impacts that are being faced by the entity and would bring the entity back to its original level of business functioning. The disaster recovery plan is composed of a number of sections that document resources and procedures to be used in the event that a disaster occurs at the Information Technology Services Locations. Each supported application or platform has a section containing specific recovery procedures. There are also sections that document the personnel that will be needed to perform the recovery tasks and an organisational structure for the recovery process. This plan will be updated on a regular basis as changes to the computing and networking systems are made. Due to the very sensitive nature of the information contained in the plan, the plan should be treated as a confidential document and should be shared with specific employees as per the specific responsibilities they have been assigned.

2.4.2 DRP scope and objectives

The DRP should inform the user about the primary focus of this document like responding to disaster, restoring operations as quickly as possible and reducing the number of decisions which must be made when, and if, a disaster occurs. It should also inform about the responsibility to keep this document current. It should be approved by appropriate authority.

The overall objectives of this plan are to protect organisation's computing resources and employees, to safeguard the vital records of which Information Technology Systems and to guarantee the continued availability of essential Information Technology services. The role of this plan is to document the pre-agreed decisions and to design and implement a sufficient set of procedures for responding to a disaster that involves the data centre and its services.

A disaster is defined as the occurrence of any event that causes a significant disruption in Information Technology capabilities. This plan assumes the most severe disaster, the kind that requires moving computing resources to another location. Less severe disasters are controlled at the appropriate management level as a part of the total plan.

The basic approach, general assumptions, and possible sequence of events that need to be followed are stated in the plan. It will outline specific preparations prior to a disaster and emergency procedures immediately after a disaster. The plan is a roadmap from disaster to recovery. Due to the nature of the disaster, the steps outlined may be skipped or performed in a different sequence. The general approach is to make the plan as threat-independent as possible. This means that it should be functional regardless of what type of disaster occurs.

For the recovery process to be effective, the plan is organised around a team concept. Each team has specific duties and responsibilities once the decision is made to invoke the disaster recovery mode. The plan represents a dynamic process that will be kept current through updates, testing, and reviews. As recommendations are completed or as new areas of concern are recognised, the plan will be revised to reflect the current IT and business environment. **The IS Auditor has to review the process followed for preparation of the DRP and assess whether it meets the requirements of the organisation and provide recommendations on any areas of weaknesses identified.**

2.4.3 Disaster recovery phases

The disaster recovery process consists of four phases which are outlined here:

- Phase 1: Disaster Assessment
- Phase 2: Disaster Recovery Activation
- Phase 3: Alternate Site/Data Centre Rebuild
- Phase 4: Return to Primary site

1. **Disaster assessment:** The disaster assessment phase lasts from the inception of the disaster until it is under control and the extent of the damage can be assessed. Co-operation with emergency services personnel is critical.
2. **Disaster recovery activation:** When the decision is made to move primary processing to another location, this phase begins. The Disaster Recovery Management Team will assemble and call upon team members to perform their assigned tasks. The most important function is to fully restore operations at a suitable location and resume normal functions. Once normal operations are established at the alternate location, Phase 2 is complete.
3. **Alternate site operation/data centre rebuild:** This phase involves continuing operations at the alternate location. In addition, the process of restoring the primary site will be performed.
4. **Return to primary site:** This phase involves the reactivation of the primary site at either the original or possibly a new location. The activation of this site does not have to be as rushed as the activation of the alternate recovery site. At the end of this phase, a thorough review of the disaster recovery process should be taken. Any deficiencies in this plan can be corrected by updating the plan.

2.4.4 Key Disaster recovery activities

The declaring of an incident/event is done by assigned personnel of management. Declaration of a disaster means:

1. Activating the recovery plan
2. Notifying team leaders
3. Notifying key management contacts
4. Redirecting information technology service to an alternate location
5. Securing a new location for the data centre

6. Ordering and configuring replacement equipment
7. Reconfiguring the network
8. Reinstalling software and data
9. Keeping management informed
10. Keeping users informed
11. Keeping the public informed

2.4.5 DRP

The DRP should contain information about the vital records details including location where it is stored, who is in charge of that record etc. It contains information about what is stored offsite such as:

1. A current copy of this disaster recovery plan.
2. Copies of install disks for all relevant software and critical software/operating system licences. These should be stored electronically rather than relying on Internet-downloadable versions. When the software is needed the same version of the software used may not be available on the Internet, or there may be Internet issues that could negatively affect large downloads or may significantly slow down the recovery process.

2.4.6 Disaster Recovery Team

The disaster recovery plan should contain details about Disaster Recovery Management Team and its sub-teams like Administration, Supplies, Public relations etc. and their respective responsibilities. The various types of responsibilities applicable in case of a disaster are explained here covering specific stages.

General Responsibilities

The IT Disaster Recovery Management Team (MGMT) is responsible for the overall co-ordination of the disaster recovery process from an Information Technology Systems perspective. The other team leaders report to this team during a disaster. In addition to their management activities, members of this team will have administrative, supply, transportation, and public relations responsibilities during a disaster. Each of these responsibilities should be headed by a member of the MGMT team.

General Activities

- Assess the damage and if necessary, declare a disaster (damage assessment forms are included in this plan)
- Co-ordinate efforts of all teams
- Secure financial backing for the recovery effort
- Approve all actions that were not pre-planned
- Give strategic direction

- Be the liaison to upper management
- Expedite matters through all bureaucracy
- Provide counselling to those employees that request or require it

After The Disaster

- Make recommendations on how the disaster recovery plan can be improved

Administrative Responsibilities

The administrative function provides administrative support services to any team requiring this support. This includes the hiring of temporary help or the reassignment of other clerical personnel.

Activities by Phase

Procedures during Disaster Recovery Activation Phase

- Notify all vendors and delivery services of change of address

Procedures during All Phases

- Process expense reports
- Account for the recovery costs
- Handle personnel problems

After The Disaster

- Make recommendations on how the disaster recovery plan can be improved

Supply Responsibilities

The supply function is responsible for co-ordinating the purchase of all needed supplies during the disaster recovery period. Supplies include all computing equipment and supplies, office supplies such as paper and pencils, and office furnishings.

Activities by Phase

Procedures during Disaster Recovery Activation Phase

- Purchase supplies required by the teams at the alternate site.

Procedures during Remote Operation/Data Centre Rebuild Phase

- Work with procurement to order replacement supplies and expedite shipments
- Ongoing distribution of supplies

Procedures during return to primary site phase

- Restock supplies at the restored site

After the disaster

- Make recommendations on how the disaster recovery plan can be improved

Public Relations Responsibilities

The public relations function will pass appropriate information about the disaster and associated recovery process to the public and to employees. Every effort should be made to give these groups reason to believe that TAMUCT is doing everything possible to minimise losses and to ensure a quick return to normalcy.

Activities by Phase

All Phases

- Ensure that employees do not talk to the media
- Control information released to the public and to employees
- Interface with organisation's Public Relations or defer to Senior Management
- Publish internal newsletters
- Keep everyone aware of recovery progress

After the Disaster

- Make recommendations on how the disaster recovery plan can be improved

Management Team Call Checklist

The disaster recovery plan should contain disaster recovery management team call checklist. It should specify the contact information about Team leader as well as team members with the details on which functionality he/she can be contacted. The disaster recovery plan should contain details about Technical support Team and its sub-teams like Hardware, Software, Network, Operations etc. and their respective responsibilities.

Hardware Responsibilities

The responsibility of the Hardware Team is to acquire (along with the Facilities Team), configure and install servers and workstations for organisational information Technology users.

Activities by Phase

Procedures during Disaster Recovery Activation Phase

- Determine scope of damage for servers and workstations
- Order appropriate equipment and supplies (co-ordinate and work with the Facilities Team for this activity)

Procedures during Remote Operation/Data Centre Rebuild Phase

- Set up servers and workstations
- Install software as necessary
- Restore data
- Install additional workstations as they arrive

Procedures during Return Home Phase

- Notify users
- Ensure data is backed up
- Relocate equipment

After the Disaster

- Make recommendations on how the disaster recovery plan can be improved

Software Responsibilities

The responsibility of the Software Team is to maintain the systems software at the alternate site and reconstruct the system software upon returning to the primary site. In addition, the Software Team will provide technical support to the other teams.

Activities by Phase

Procedures during Disaster Recovery Activation Phase

- Provide technical support to the other teams
- Build servers and workstations
- Reinstall and configure systems at the primary site
- Test the hardware and software
- Work with appropriate vendors to assist in recovery
- Verify that the systems are performing as expected

Procedures during Remote Operation/Data Centre Rebuild Phase

- Provide technical support to the other teams
- Build servers and workstations
- Reinstall and configure systems at the primary site
- Test the hardware and software
- Work with appropriate vendors to assist in recovery
- Verify that the systems are performing as expected

Procedures during Return Home Phase

- Provide technical support to the other teams
- Verify that the system is performing as expected

After the Disaster

- Make recommendations on how the disaster recovery plan can be improved

Network Responsibilities

The Network Team is responsible for preparing for voice and data communications to the alternate location data centre and restoring voice and data communications at the primary site.

Activities by Phase

Procedures during disaster recovery activation phase

- Determine the requirements for voice and data communications
- Install the network including lines, routers, switches, controllers and other communications equipment at the alternate location data centre
- Test the network.

Procedures during Remote Operation/Data Centre Rebuild Phase

- Operate the backup network
- When the replacement equipment arrives at the primary site, install it

Procedures during Relocation Home Phase

- Support the primary site network
- Dismantle the alternate location data centre network

After the Disaster

- Make recommendations on how the disaster recovery plan can be improved

Operations Responsibilities

The operations responsibilities include the daily operation of computer services and management of all backup tapes. When a disaster is declared, the team must secure the correct tapes for transport to the alternate location. Once operations are established at the alternate location, arrangements must be made with an offsite storage service.

Activities by Phase

Procedures during Disaster Recovery Activation Phase

- Inventory and select the correct backup tapes
- Transport the tapes to the alternate data centre
- Assist all teams in restoring the production environment at the alternate data centre

Procedures during Remote Operation/Data Centre Rebuild Phase

- Establish a production schedule at the alternate location
- Run the daily schedule at the alternate location
- Perform system and production backups at the alternate location
- Assist other teams in preparing the primary site
- Establish offsite storage at the alternate location

Procedures during Return Home Phase

- Perform system and production backups
- Inventory all tapes at the alternate data centre
- Transport all tapes from the alternate data centre to the primary site

After the Disaster

- Make recommendations on how the disaster recovery plan can be improved

Technical Support Team Call Checklist

The disaster recovery plan should contain Disaster Recovery Technical Support Team Call Checklist. It should specify the contact information about Team leader as well as team members with the details on which functionality he/she can be contacted. The disaster recovery plan should contain details about Facility Team and its sub-teams like Salvage team, new data centre, new hardware team etc. and their respective responsibilities.

Salvage Responsibilities

The Salvage Team is responsible for minimising the damage at the primary site and to work with the insurance company for settlement of all claims. This depends on a quick determination of what equipment is salvageable and what is not. Repair and replacement orders will be filed for what is not in working condition. This team is also responsible for securing the disaster recovery data centre.

Activities by Phase

Procedures during Disaster Recovery Activation Phase

- Establish the command centre
- Assist in the immediate salvage operations
- Contact Insurance representatives
- Inventory all equipment in the data centre. If necessary, involve the vendors.

Procedures during Remote Operation/Data Centre Rebuild Phase

- Salvage equipment and supplies
- Settle property claims with the insurance company
- Provide for security at the data centre

After the Disaster

- Make recommendations on how the disaster recovery plan can be improved

New Data Centre Responsibilities

The New Data Centre Team is responsible for locating the proper location for a new data center and overseeing the construction of it. This includes the environmental and security controls for the room.

Activities by Phase

Procedures during Remote Operation/Data Centre Rebuild Phase

- Determine the requirements for a new data centre
- Work with contractors and university staff on the details
- Oversee the construction of the new data centre

Procedures during Return Home Phase

- Ensure that all controls are working as designed

After the Disaster

- Make recommendations on how the disaster recovery plan can be improved

New Hardware Responsibilities

The New Hardware Team is responsible for ordering replacement hardware for equipment damaged in the disaster and installing it in the new or rebuilt data centre. Depending on the age of the damaged hardware, replacement may not be one-for-one. All types of hardware are to be handled, including:

1. Servers
2. Printers
3. Switches, Routers, Hubs
4. Work stations
5. Environmental systems
6. UPS Equipment

Activities by Phase

Procedures during Disaster Recovery Activation Phase

- Obtain a list of damaged and destroyed equipment

Procedures during Remote Operation/Data Centre Rebuild Phase

- Determine what new hardware should be ordered
- Order new hardware
- Arrange for installation and testing of the new hardware

After the Disaster

- Make recommendations on how the disaster recovery plan can be improved

Resumption of Normal Operations

Once the threat has passed, equipment has been repaired or replaced or a new primary site has been built and stocked, the disaster recovery team will assess the situation, declare the disaster over and resume normal operations

2.5 Documentation: BCP Manual and BCM Policy

All documents that form the BCM are to be subject to document control and record control processes. The following documents (representative only) are classified as being part of the business continuity management system:

- The business continuity policy.
- The business continuity management system.
- The business impact analysis report.
- The risk assessment report.
- The aims and objectives of each function.
- The activities undertaken by each function.
- The business continuity strategies.
- The overall and specific incident management plans.
- The business continuity plans.
- SLA with alternate site/mirror site with switchover plans.
- Change control, preventative action, corrective action, document control and record control processes

- Local Authority Risk Register;
- Exercise schedule and results;
- Incident log; and
- Training Programme

To provide evidence of the effective operation of the BCM, records demonstrating the operation should be retained as per policy of the organisation and as per applicable laws, if any. These records also include reference to all business interruptions and incidents, irrespective of the nature and length of disruption. This also includes general and detailed definition of requirements as described in developing a BCP. In this, a profile is developed by identifying resources required to support critical functions, which include hardware (mainframe, data and voice communication and personal computers), software (vendor supplied, in-house developed, etc.), documentation (user, procedures), outside support (public networks, DP services, etc.), facilities (office space, office equipment, etc.) and personnel for each business unit.

2.5.1 BCM Policy

While developing the BCM policy, the organisation should consider defining the scope, BCM principles, guidelines and applicable standards for the organisation. They should consider all relevant standards, regulations and policies that have to be included or can be used as benchmark. The objective of this policy is to provide a structure through which:

- Critical services and activities undertaken by the organisation will be identified.
- Plans will be developed to ensure continuity of key service delivery following a business disruption, which may arise from the loss of facilities, personnel, IT and/or communication or failure within the supply and support chains.
- Invocation of incident management and business continuity plans can be managed.
- Incident Management Plans and BCP are subject to ongoing testing, revision and updating as required.
- Planning and management responsibility are assigned to members of the relevant senior management team.

The BCM policy defines the processes of setting up activities for establishing a business continuity capability and the ongoing management and maintenance of the business continuity capability. The set-up activities incorporate the specification, end-to-end design, build, implementation and initial exercising of the business continuity capability. The ongoing maintenance and management activities include embedding business continuity within the organisation, exercising plans regularly, and updating and communicating them, particularly when there is significant change in premises, personnel, process, market, technology or organisational structure.

2.5.2 BCP Manual

An incident or disaster affecting critical business operations can strike at any time. Successful organisations have a comprehensive BCP Manual, which ensures process readiness, data and system availability to ensure business continuity. A BCP manual is a documented description of actions to be taken, resources to be used and procedures to be followed before, during and after an event that severely disrupts all or part of the business operations. A BCP manual consists of

the Business Continuity Plan and the Disaster Recovery Plan. The primary objective of preparing BCP manual is to provide reasonable assurance to senior management of organisation about the capability of the organisation to recover from any unexpected incident or disaster affecting business operations and continue to provide services with minimal impact. Further, the BCP should be comprehensive and anticipate various types of incident or disaster scenarios and outline the action plan for recovering from the incident or disaster with minimum impact and ensuring continuous availability of all key services. The BCP Manual is expected to specify the responsibilities of the BCM team, whose mission is to establish appropriate BCP procedures to ensure the continuity of organisation's critical business functions. In the event of an incident or disaster affecting any of the functional areas, the BCM Team serves as visioning teams between the functional area(s) affected and other departments providing support services.

Elements of BCP Manual

The plan will contain the following elements:

1. **Purpose of the plan:** Included in this section should be a summary description of the purpose of the manual. It should be made clear that the manual does not address recovery from day-to-day operational problems. Similarly, it must be stressed that the manual does not attempt to foresee all possible disasters, but rather provides a framework within which management can base recovery from any given disaster.
2. **Organisation of the manual:** A brief description of the organisation of the manual, and the contents of each of the major sections, will provide the reader with the direction to the relevant section of the manual in an emergency situation. Any information which is external to the manual but will be required in an emergency should be identified in this section.
3. **Disaster definitions:** It may assist the user of the manual if a definition of disaster classification is provided, together with an identification of the relevance of the plan to that situation. Four types of classification can generally be used:
    - **Problem/Incident:** Event or disruptions that cause no significant damage.
    - **Minor disaster:** Event or disruption that causes limited financial impact,
    - **Major disaster:** Event or disruptions that cause significant impact and may have an effect on outside clients.
    - **Catastrophic disaster:** Event or disruption that has significant impact and adversely affect the organisation’s “going concern” status

The BCP manual of each organisation is expected to classify disasters, after taking into account the size and nature of its business and the time and cost associated to each kind of disaster should be defined as per the requirement of the individual organisation. It should be noted, however, that development of a plan based on each classification is not recommended. The need to invoke the plan should be determined by the length and associated cost of the expected outage and not the classification of the disaster, although there is a direct correlation. These definitions will be most useful for communication with senior management.

4. **Objectives of the plan:** The objectives of the manual should be clearly stated in the introductory section. Typically, such objectives include:

- Safety/security all personnel. The paramount objective of a BCP is to ensure the safety and security of people (both employees and others who may be affected in the event of a disaster). The safeguarding of assets/data is always a secondary objective.
- The reduction of confusion in an emergency
- The identification of critical application systems and/or business functions
- The identification of all resources, including personnel, required to recover the critical business functions
- The identification of alternative means of ensuring that the critical business functions are performed and
- The establishment of a workable plan to recover the critical business functions, and subsequently resume normal operations, as quickly as possible after a disaster.

The list should be expanded as necessary to meet the requirements of any given plan.

5. **Scope of the plan:** In order that there is no confusion as the situations in which the plan will apply, the scope of the plan must be clearly identified. Any limitations must be explained.
6. **Plan approach/recovery strategy:** A step by step summary of the approach adopted by the plan should be presented. For ease of reference, it may be good to provide this overview by means of a schematic diagram. In particular, it may be useful to set up the recovery process as a project plan in this section.
7. **Plan administration:** The introductory section should also identify the person or persons, responsible for the business continuity plan manual, and the expected plan review cycles. These persons will be responsible for issuing revisions which will ensure that the plan remains current. Because the manual will include staff assignments, it is also advisable that the personnel or human resource function accept responsibility for notifying the plan administrators of all personnel changes which must be reflected in the plan.
8. **Plan management:** Following a disaster, the normal reporting channels and lines of management are unlikely to be strictly adhered to. During a disaster, reporting by exception may be the only feasible way to operate. This does not however negate the requirement for formalised management. The management responsibilities and reporting channels to be observed, during disaster recovery should be clearly established in advance.
9. **Disaster notification and plan activation procedures:** The procedures represent the first steps to be followed when any disaster occurs. It is recommended that the procedures be written in a task oriented manner and provide a logical flow to enable ease of management.

2.6 Data backup, Retention and Restoration practices

2.6.1 Back upstrategies

Backup refers to making copies of the data so that these additional copies may be used to restore the original data after a data loss. Various backup strategies are:

- **Dual recording of data:** Under this strategy, two complete copies of the database are maintained. The databases are concurrently updated.
- **Periodic dumping of data:** This strategy involves taking a periodic dump of all or part of the database. The database is saved at a point in time by copying it onto some backup storage medium – magnetic tape, removable disk, Optical disk. The dump may be scheduled.
- **Logging input transactions:** This involves logging the input data transactions which cause changes to the database. Normally, this works in conjunction with a periodic dump. In case of complete database failure, the last dump is loaded and reprocessing of the transactions are carried out which were logged since the last dump.
- **Logging changes to the data:** This involves copying a record each time it is changed by an update action. The changed record can be logged immediately before the update action changes the record, immediately after, or both.

Apart from database backup strategies as mentioned above, it is important to implement e-mail and personal files backup policies. The policy can be like burning DVDs with the folders and documents of importance periodically to more detailed and automated functions. The choice depends and varies with the size, nature and complexity of the situation. For example, individuals are responsible for taking backups of personal files and folders. However, a policy may be there whereby individual users may transfer personal files and folders from the PC to an allocated server space. The data so transferred in the server will be backed up by the IT department as a part of their routine backup. E-mail backups should necessarily include the address book backup. However, the most important and critical part of the backup strategy is to include a restoration policy. Restoration of the data from the backup media and devices will ensure that the data can be restored in time of emergency; else a failed backup is a double disaster. The restoration should be done for all backups at least twice a year.

Types of Backup

When the backups are taken of the system and data together, they are called total system's backup. An organisation has to choose the right type of backup for each of the critical components of IS and data to meet specific business requirements. The various types of backups are:

- **Full Backup:** A full backup captures all files on the disk or within the folder selected for backup. With a full backup system, every backup generation contains every file in the backup set. However, the amount of time and space such a backup takes prevents it from being a realistic proposition for backing up a large amount of data.
- **Incremental Backup:** An incremental backup captures files that were created or changed since the last backup, regardless of backup type. This is the most economical method, as only the files that changed since the last backup are backed up. This saves a lot of backup time and space. Normally, incremental backup are very difficult to restore. One will have to start with recovering the last full backup, and then recovering from every incremental backup taken since.

- **Differential Backup:** A differential backup stores files that have changed since the last full backup. Therefore, if a file is changed after the previous full backup, a differential backup takes less time to complete than a full backup. Comparing with full backup, differential backup is obviously faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved. Restoring from a differential backup is a two-step operation: Restoring from the last full backup; and then restoring the appropriate differential backup. The downside to using differential backup is that each differential backup probably includes files that were already included in earlier differential backups.
- **Mirror backup:** A mirror backup is identical to a full backup, with the exception that the files are not compressed in zip files and they cannot be protected with a password. Mirror backup is most frequently used to create an exact copy of the backup data.

2.6.2 Recovery strategies

The backup plan is intended to restore operations quickly so that information system function can continue to service an organisation, whereas, recovery plans set out procedures to restore full information system capabilities. Recovery plan should identify a recovery team that will be responsible for working out the specifics of the recovery to be undertaken. The plan should specify the responsibilities of the various departments and provide guidelines on priorities to be followed. The plan might also indicate which applications are to be recovered first. Members of the recovery team must understand their responsibilities. Again, the problem is that they will be required to undertake unfamiliar tasks. Periodically, they must review and practice executing their responsibilities so they are prepared should a disaster occur. If employees leave the organisation, new employees must be assigned the responsibility immediately and briefed about their responsibilities. The recovery strategies for various types of information systems are outlined here.

Strategies for Networked Systems

Most organisations use networked systems. There is heavy dependence on main server and network in case of networked systems. The recovery strategy would vary depending on the type of network architecture and implementation. For example, LANs can be implemented in two main architectures:

LAN Systems

Peer-to-Peer: Each node has equivalent capabilities and responsibilities. For example, five PCs can be networked through a hub to share data.

Client/Server: Each node on the network is either a client or a server. A client can be a PC or a printer where a client relies on a server for resources. A LAN's topology, protocol, architecture, and nodes will vary depending on the organisation. Thus, contingency solutions for each organisation will be different. Listed below are some of the strategies for recovery of LANs.

1. **Eliminating Single Points of Failure (SPOC):** When developing the LAN contingency plan, the organisation should identify single points of failure that affect critical systems or processes outlined in the Risk Assessment. These single points of failures are to be eliminated by providing alternative or redundant equipment.

2. **Redundant Cabling and Devices:** Contingency planning should also cover threats to the cabling system, such as cable cuts, electromagnetic and radiofrequency interference, and damage resulting from fire, water, and other hazards. As a solution, redundant cables may be installed when appropriate. For example, it might not be cost-effective to install duplicate cables to every desktop. However, it might be cost-effective to install a redundant cable between floors so that hosts on both floors could be reconnected if the primary cable were cut. Contingency planning also should consider network connecting devices such as hubs, switches, bridges, and routers.

3. **Remote Access:** Remote access is a service provided by servers and devices on the LAN. Remote access provides a convenience for users working off-site or allows for a means for servers and devices to communicate between sites.

Remote access can be conducted through various methods, including dialup access and virtual private network (VPN). Remote access may serve as allocation that can access the corporate data even when they are not in a position to reach the physical premises due to some calamity. If remote access is established as a contingency strategy, data bandwidth requirements should be identified and used to scale the remote access solution. Additionally, security controls such as one-time passwords and data encryption should be implemented, if the communication traffic contains sensitive information.

Wireless LANs

Wireless local area networks can serve as an effective contingency solution to restore network services following a wired LAN disruption. Wireless networks do not require the cabling infrastructure of conventional LANs; therefore, they may be installed quickly as an interim or permanent solution. However, wireless networks broadcast the data over a radio signal, enabling the data to be intercepted. When implementing wireless network, security controls, such as data encryption, should be implemented, if the sensitive information is to be communicated.

Strategies for Distributed Systems

A distributed system is an interconnected set of multiple autonomous processing elements, configured to exchange and process data to complete a single business function. To the user, a distributed system appears to be a single source. Distributed systems use the client-server model to make the application more accessible to users in different locations. Distributed systems are implemented in environments in which clients and users are widely dispersed. These systems rely on LAN and WAN resources to facilitate user access and the elements comprising the distributed system require synchronisation and co-ordination to prevent disruptions and processing errors. A common form of distributed systems is a large database management system (DBMS) that supports organisation wide business functions in multiple geographic locations. In this type of application, data is replicated among servers at each location, and users access the system from their local server. The contingency strategies for distributed system reflect the system's Reliance Nolan and WAN availability. Based on this fact, when developing a distributed system contingency strategy, the following methods applicable to system backups should be considered for decentralised systems. In addition, a distributed system should consider WAN communication link redundancy and possibility of using Service Bureaus and Application Service Providers (ASPs).

Strategies for Data communications

i. **Dial-up:** Using Dial-up as a backup to normal leased or broadband communications lines remains the most popular means of backing up wide-area network communications in an emergency. This approach requires compatible modems at each remote site and at the recovery location. Ideally, the modems should be full duplex modems which will permit transmission and receipt down the same line. The half-duplex option will require two telephone lines for each data line lost.

ii. **Circuit Extension:** Circuit extension techniques are usually applied to high bandwidth communications services, such as high speed leased lines. This technique builds redundancy into the client's network, by including the recovery site as a defined and serviced node. This is by, where the communications from the remote sites can be directed to the primary site or the recovery site from the carrier's central office. This is effective duplication of equipment and facilities, but with some potential for sharing the costs of the equipment at the recovery site.

iii. **On-demand service from the carriers:** Many carriers now offer on-demand services which provide the mechanisms to switch communications to the recovery site from the primary site on client notification.

iv. **Diversification of services:** The use of diverse services provides the best solutions to the loss of a carrier central office. Diversity can be achieved in a number of manners, including: Use of more than one carrier on a regular basis. If the organisation uses two or more carriers, it will likely pay above the odds for its regular service and require investment in some additional equipment. For this approach to communications recovery to work, there must also be some redundancy accommodated following any carrier outage.

v. **Microwave communications:** The regular communications can be backed up by the use of microwave communications. This could be used to: backup communications from the central office to the primary site, in case of breakage in the land lines; backup communications from the central office to the recovery centre; or a backup link from a company controlled communications centre direct to the recovery centre.

vi. **VSAT (Very Small Aperture Terminal) based satellite communications:** Companies are increasingly looking to VSAT communications as a cost effective means of communicating large volumes of information. This technique could similarly be used to back up the primary carrier service. The use of this technology requires VSAT terminals to be installed at each remote location and at the recovery centre if it does not currently provide such a service.

Strategies for Voice Communications

Many of the techniques and concerns above relate to voice communications as wells data, and this will continue with the expansion of ISDN services for integrated voice and data communications. Other techniques available for voice recovery include:

I. **Cellular phone backup:** If the regular voice system is inoperative, key employees can be provided with cellular phones as a backup. Given that cellular phones are not run by the major carriers from the same central offices, this also provides coverage for the loss

of the central office. Such phones could also be used on an on-going basis and could be used to balance the load on the main PBX switch. Cellular services can also be extended to data and facsimile transmission.

ii. **Carrier call rerouting systems:** Most of the major carriers now provide customers with call rerouting services such that all calls to a given number can be rerouted to another number temporarily. While this will not be possible in the case of a carrier outage, it can be used for the rerouting of critical business communications following a disaster at a client's offices. Calls can be rerouted to call management service, for example, to support the client in the interim.

2.7 Types of recovery and alternative sites

The traditional focus of BCP/DRP was the recovery of the corporate computer system, which was almost always a mainframe or large minicomputer. Mainframe centric disaster recovery plans often concentrated on replacing an inaccessible or non-functional mainframe with compatible hardware. A backup site or work area recovery (alternate processing site) site is a location where an entity can easily function out of immediately following a disaster. This is an integral part of a DRP or BCP. Types of alternate processing sites are outlined along with some of the widely adopted strategies for centralised system recovery.

2.7.1 Mirror Site/ Active Recovery Site

Mirror site

The single most reliable system backup strategy is to have fully redundant systems called an active recovery or mirror site. While most companies cannot afford to build and equip two identical data centres, those companies that can afford to do so have the ability to recover from almost any disaster. This is the most reliable and also the most expensive method of systems recovery.

Hot Site

A dedicated contingency centre, or 'hot site' is a fully equipped computer facility with electrical power, heating, ventilation and air conditioning (HVAC) available for use in the event of a subscriber's computer outage. These facilities are available to a large number of subscribers on a membership basis and use of site is on a 'first come, first served' basis. In addition to the computer facility, these facilities offer an area of general office space and computer ready floor space on which the users can build their own long-term recovery configuration. Some of the vendors also offer remote operations facilities for use in tests or emergency. Where the recovery center is in a city other than the subscriber's home location, this can be used to reduce the need to transport staff and resources.

A hot site is a duplicate of the original site of the organisation, with full computer systems as well as near-complete backups of user data. Real time synchronisation between the two sites may be used to completely mirror the data environment of the original site using wide area network links and specialised software. Following a disruption to the original site, the hot site exists so that the organisation can relocate with minimal losses to normal operations. Ideally, a hot site will be up and running within a matter of hours or even less. Personnel may still have to be moved to the

hot site so it is possible that the hot site may be operational from a data processing perspective before staff has relocated. The capacity of the hot site may or may not match the capacity of the original site depending on the organisation's requirements. This type of backup site is the most expensive to operate. Hot sites are popular with organisations that operate real time processes such as financial institutions, government agencies and ecommerce providers.

Cold Site

A cold site is the least expensive type of backup site for an organisation to operate. It does not include backed up copies of data and information from the original location of the organisation, nor does it include hardware already set up. The lack of hardware contributes to the minimal start-up costs of the cold site, but requires additional time following the disaster to have the operation running at a capacity close to that prior to the disaster.

Warm Site

A warm site is a compromise between hot and cold. These sites will have hardware and connectivity already established, though on a smaller scale than the original production site or even a hot site. Warm sites will have backups on hand, but they may not be complete and may be between several days and a week old. An example would be backup tapes sent to the warm site by courier.

2.7.2 Offsite data protection

Offsite data protection is the strategy of sending critical data out of the main location as a part of DRP. Data is usually transported off-site using removable storage media such as magnetic tape or optical storage. Data can also be sent electronically via a remote backup service, which is known as electronic vaulting or e-vaulting. Sending backups off-site ensures systems and servers can be reloaded with the latest data in the event of a disaster, accidental error, or system crash. Sending backups off-site also ensures that there is a copy of pertinent data that isn't stored on-site. Off-site backup services are convenient for companies that backup pertinent data on a daily basis. The different types of Offsite Data Protection are outlined here.

Data Vaults

Backups are stored in purpose built vaults. There are no generally recognised standards for the type of structure which constitutes a vault. Commercial vaults fit into three categories:

1. Underground vaults
2. Free-standing dedicated vaults
3. Insulated chambers sharing facilities

Hybrid on-site and off-site vaulting

Hybrid on-site and off-site data vaulting, sometimes known as Hybrid Online Backup, involve a combination of Local backup for fast backup and restore, along with Off-site backup for protection against local disasters. This ensures that the most recent data is available locally in the event of need for recovery, while archived data that is needed much less often is stored in the cloud.

Hybrid Online Backup works by storing data to local disk so that the backup can be captured at high speed, and then either the backup software or a D2D2C (Disk to Disk to Cloud) appliance encrypts and transmits data to a service provider. Recent backups are retained locally, to speed data recovery operations. There are a number of cloud storage appliances on the market that can be used as a backup target, including appliances from CTERA Networks, Naquin, StorSimple and Twin Strata.

Aternate Site Selection Criteria					
SITE	COST	HARDWARE EQUIPMENT	TELECOMM UNICATIONS	SET UP TIME	LOCATION
COLD SITE	Low	None	None	Long	Fixed
WARM SITE	Medium	Partial	Partial/ Full	Medium	Fixed
HOT SITE	Medium/ High	Full	Full	Short	Fixed
MOBILE SITE	High	Dependent	Dependent	Dependent	Not Fixed
MIRRORED SITE	High	Full	Full	None	Fixed

2.8 System Resiliency Tools and Techniques

2.8.1 Fault Tolerance

Fault-tolerance is the property that enables a system (often computer-based) to continue operating properly in the event of the failure of (or one or more faults within) some of its components. The basic characteristics of fault tolerance require:

1. No single point of failure
2. No single point of repair
3. Fault isolation to the failing component
4. Fault containment to prevent propagation of the failure
5. Availability of reversion modes

In addition, fault tolerant systems are characterised in terms of both planned service outages and unplanned service outages. These are usually measured at the application level and not just at a hardware level. The figure of merit is called availability and is expressed as a percentage. A five nines system would therefore statistically provide 99.999% availability. A spare component addresses first fundamental characteristic of fault-tolerance in three ways:

i. **Replication:** Providing multiple identical instances of the same system or subsystem, directing tasks or requests to all of them in parallel, and choosing the correct result on the basis of a quorum;

ii. **Redundancy:** Providing multiple identical instances of the same system and switching to one of the remaining instances in case of a failure (failover);

iii. **Diversity:** Providing multiple *different* implementations of the same specification and using them like replicated systems to cope with errors in a specific implementation.

2.8.2 Redundant array of inexpensive disks (RAID)

RAID provides fault tolerance and performance improvement via hardware and software solutions. It breaks up the data to write it in multiple disks to improve performance and / or save large files. There are many methods of RAID which are categorised into several levels. There are various combinations of these approaches giving different trade-offs of protection against data loss, capacity, and speed.

RAID levels: Levels 0, 1, and 5 are the most commonly found, and cover most requirements. Generally, most organisations use RAID-1 to RAID-5 for data redundancy.

Electronic vaulting: Electronic vaulting is a backup type where the data is backed up to an offsite location. The data is backed up, generally, through batch process and transferred through communication lines to a server at an alternate location.

Remote journaling: Remote journaling is a parallel processing of transactions to an alternate site, as opposed to batch dump process like electronic vaulting. The alternate site is fully operational at all times and introduces a very high level of fault tolerance.

Database shadowing: Database shadowing is the live processing of remote journaling, but creates even more redundancy by duplicating the database sites to multiple servers.

2.9 Insurance coverage for BCP

The purpose of insurance is to spread the economic cost and the risk of loss from an individual or business to a large number of people. This is accomplished through the use of an insurance policy. Policies are contracts that obligate the insurer to indemnify the policyholder or some third party from specific risks in return for the payment of a premium. Adequate insurance coverage is a key consideration when developing a BCP and performing a risk analysis. Most insurance agencies specialising in business interruption coverage can provide the organisation with an estimate of anticipated business interruption costs. Most business interruption coverage includes lost revenues following disaster. Extra expense coverage includes all additional expenses until normal operations can be resumed.

2.9.1 Coverage

Insurance policies usually can be obtained to cover the following resources:

- **Equipment:** Covers repair or acquisition of hardware. It varies depending on whether the equipment is purchased or leased.
- **Facilities:** Covers items such as reconstruction of a computer room, raised floors, special furniture.
- **Storage media:** Covers the replacement of the storage media plus their contents – data files, programmes, documentation.
- **Business interruption:** Covers loss in business income because an organisations is unable to trade.

- **Extra expenses:** Covers additional costs incurred because an organisation is not operating from its normal facilities.
- **Valuable papers:** Covers source documents, pre-printed reports, and records documentation, and other valuable papers.
- **Accounts receivable:** Covers cash-flow problems that arise because an organisation cannot collect its accounts receivable promptly.
- **Media transportation:** Covers damage to media in transit.
- **Malpractice, errors:** Covers claims against an organisation by its customers, and omission e.g., claims and omission made by the clients of an outsourcing vendor or service bureau.

2.9.2 Kinds of Insurance

Insurance is generally divided into two general classes based upon whether the insured is the injured party. Lawyers call these two divisions first-party and third-party insurance. First-party insurance identifies claims by the policyholder against their own insurance. Third-party insurance is designed to protect against claims made against the policyholder and his insurer for wrongs committed by the policyholder. The most common form of first-party insurance is property damage, while the most common form of third-party insurance is liability.

(a) First-party Insurances: Property Damages

Perhaps the oldest insurance in the world is that associated with damage to property. It is designed to protect the insured against the loss or destruction of property. It is offered by the majority of all insurance firms in the world and uses time-tested forms, the industry term for a standard insurance contract accepted industry-wide. This form often defines loss as “physical injury to or destruction of tangible property” or the “loss of use of tangible property which has not been physically injured or destroyed.” Such policies are also known as all risks, defined risk, or casualty insurance.

(b) First-party Insurances: Business Interruption

If an insured company fails to perform its contractual duties, it may be liable to its customers for breach of contract. One potential cause for the inability to deliver might be the loss of information system, data or communications. Some in business and the insurance industry have attempted to mitigate this by including information technology in business recovery/disaster plans. As a result, there has emerged a robust industry in hot sites for companies to occupy in case of fire, flood, earthquake or other natural disaster. Disaster recovery has become a necessity in the physical world. While the role of disaster recovery is well understood in business, the insurance industry was slow to accept the indemnity role relative to insuring data in a business interruption liability insurance context. Insurers are generally aggressive in limiting their own liability and have, in a number of instances, argued that a complete cessation of business is necessary to claim damage.

(c) Third-party Insurance: General Liability

Third party insurance is designed to protect the insured from claims of wrongs committed upon others. It is in parts based on the legal theory of torts. Torts are civil wrongs which generally fit into three categories – intentional, negligent and strict liability. Intentional torts are generally excluded from liability insurance policies because they are foreseeable and avoidable by the insured. Strict liability torts, such as product liability issues, are generally covered under specialised liability insurance. Generally liability policies include comprehensive, umbrella and excess liability policies. Insured parties are exposed to the risk of liability whenever they violate some duty imposed on, or expected of, parties' relative to each other or society in general. In the cyber environment this can take many forms. If the insured's computer damages another party's computer, data connectivity, then the insured may be held liable. A company might be held liable if the computer system was used in connection with a denial-of-service attack. The insured may be also held liable for failing to protect adequately the privacy interests of parties who have been entrusted information to the care of the insured.

(iv) Third-party Insurance: Directors and Officers

Errors and Omissions (E&O) insurance is protection from liability arising from a failure to meet the appropriate standard of care for a given profession. Two common forms of E & O insurance are directors and officers, and Professional liability. Directors and officers insurance is designed to protect officers of companies, as individuals, from liability arising from any wrongful acts committed in the course of their duties as officers. These policies usually are written to compensate the officer's company for any losses payable by the company for the acts of its officers.

2.10 Summary

We can summarize the following key concepts covered in this chapter:

- The development of a Business Continuity Plan can be done with the support of BCP Policy existing in an organisation. BCP Policy sets the scope of the plan. Development of BCP involves planning BCP as a project includes conducting a Business Impact Analyses, Risk Assessment, testing of the BCP, providing training and awareness and continuous maintenance of the BCP Plan.
- Contingency planning encompass Incident Management Planning, Disaster Recovery Planning and Business Continuity Planning.
- The hierarchy for invoking a Business Continuity Plan are: Incident Handling and Response→Disaster Recovery → Business Continuity.
- Business Continuity Management would contain the following minimum documents:
    - o Business Continuity Policy which documents the scope for the Business Continuity
    - o Business Continuity Manual which documents the step by step process to achieve Business Continuity and details of relevant contacts.
- Backup and Recovery Strategies, Types of Alternative Sites, system resiliency tools and techniques etc., are some strategies which are considered in developing a Business Continuity Plan.

- Insurance is a mode of transferring the risk that arises due to the threats to the Business Continuity. The various types of insurance and coverage have been discussed in this chapter.

2.11 Questions

1. Which of the following control concepts should be included in a complete test of disaster recovery procedures?
   A. Rotate recovery managers
   B. Invite client participation
   C. Involve all technical staff
   D. Install locally stored backup
2. An advantage of the use of hot sites as a backup alternative is:
   A. The costs related with hot sites are low
   B. That hot sites can be used for a long amount of time
   C. That hot sites do not require that equipment and systems software be compatible with the primary installation being backed up
   D. That hot sites can be made ready for operation within a short span of time
3. All of the following are security and control concerns associated with disaster recovery procedures EXCEPT:
   A. Loss of audit trail
   B. Insufficient documentation of procedures
   C. Inability to restart under control
   D. Inability to resolve system deadlock
4. Which of the following business recovery strategies would require the least expenditure of funds?
   A. Warm site
   B. Empty shell
   C. Hot site
   D. Reciprocal agreement
5. Which of the following is NOT a feature of an uninterruptible power supply (UPS)?
   A. It provides electrical supply to a computer in the event of a power failure.
   B. It system is an external piece of equipment or can be built into the computer itself.
   C. It should function to allow an orderly computer shutdown.
   D. It uses a greater wattage into the computer to ensure enough power is available.

6. Which of the following would warranty a quick continuity of operations when the recovery time window is short?

   A. A duplicated back-up in an alternate site

   B. Duplicated data in a remote site

   C. Transfer of data the moment a contingency occurs

   D. A manual contingency procedure

7. For which of the following applications would rapid recovery be MOST crucial?

   A. Point-of-sale

   B. Corporate planning

   C. Regulatory reporting

   D. Departmental chargeback

8. Which of the following principles must exist to ensure the viability of a duplicate information processing facility?

   A. The site is near the primary site to ensure quick and efficient recovery is achieved.

   B. The workload of the primary site is monitored to ensure adequate backup is complete.

   C. The site contains the most advanced hardware available from the chosen vendor.

   D. The hardware is tested when it is established to ensure it is working properly.

9. While reviewing the business continuity plan of an organisation, the IS auditor observed that the organisation's data and software files are backed up on a periodic basis. Which characteristic of an effective plan does this demonstrate?

   A. Deterrence

   B. Mitigation

   C. Recovery

   D. Response

10. As updates to an online order entry system are processed, the updates are recorded on a transaction tape and a hard copy transaction log. At the end of the day, the order entry files are backed up onto tape. During the backup procedure, the disk drive malfunctions and the order entry files are lost. Which of the following are necessary to restore these files?

    A. The previous day's backup file and the current transaction tape

    B. The previous day's transaction file and the current transaction tape

    C. The current transaction tape and the current hardcopy transaction log

    D. The current hardcopy transaction log and the previous day's transaction file

2.12 Answers and Explanations

1. A. Recovery managers should be rotated to ensure the experience of the recovery plan is spread. Clients may be involved but not necessarily in every case. Not all technical staff should be involved in each test. Remote or off-site backup should always be used.

2. D. Hot sites can be made ready for operation normally within hours. However, the use of hot sites is expensive, should not be considered as a long-term solution and does require that equipment and systems software be compatible with the primary installation being backed up.

3. D. The inability to resolve system deadlock is a control concern in the design of database management systems, not disaster recovery procedures. All of the other choices are control concerns associated with disaster recovery procedures.

4. D. Reciprocal agreements are the least expensive because they usually rely on a gentlemen's agreement between two firms.

5. D. A UPS typically cleanses the power to ensure wattage into the computer remains consistent and does not damage the computer. All other answers are features of a UPS.

6. D. A quick continuity of operations could be accomplished when manual procedures for a contingency exist. Choices A, B and C are options for recovery.

7. A. A point-of-sale system is a critical online system that when inoperable will jeopardise the ability of a company to generate revenue and properly track inventory.

8. B. Resource availability must be assured. The workload of the site must be monitored to ensure that availability for emergency backup use is not impaired. The site chosen should not be subject to the same natural disaster as the primary site. In addition, a reasonable compatibility of hardware/software must exist to serve as a basis for backup. The latest or newest hardware may not adequately serve this need. Testing the site when established is essential, but regular testing of the actual backup data is necessary to ensure the operation will continue to perform as planned.

9. B. An effective business continuity plan includes steps to mitigate the effects of a disaster. To have an appropriate backup plan, an organisation should have a process capability established to restore data and files on a timely basis, mitigating the consequence of a disaster. An example of deterrence is when a plan includes installation of firewalls for information systems. An example of recovery is when a plan includes an organisation's hot site to restore normal business operations.

10. A. The previous day's backup will be the most current historical backup of activity in the system. The current day's transaction file will contain all of the day's activity. Therefore, the combination of these two files will enable full recovery up to the point of interruption.

CHAPTER 3: AUDIT OF BUSINESS CONTINUITY PLAN

Learning Objectives

This chapter deals with the regulatory requirements that make it mandatory for an organisation to have Business Continuity Management. Best practices frameworks such as COBIT can be used by adapting it as per organisation requirements to achieve effective Business Continuity Management. This chapter provides details of audit procedures that are to be followed by the IS Auditor. The audit is performed to provide assurance to management on the availability of the required controls which mitigate identified risks. A good understanding of the concepts covered in Chapters 1 to 3 will help DISAs to provide assurance and consulting services in the area of BCM, BCP and DRP.

3.1 Introduction

A business continuity plan audit is a formalised method for evaluating how business continuity processes are being managed. The goal of an audit is to determine whether the plan is effective and in line with the company's objectives. A business continuity plan audit should define the risks or threats to the success of the plan and test the controls in place to determine whether or not those risks are acceptable. An audit should also quantify the impact of weaknesses of the plan and offer recommendations for business continuity plan improvements.

3.2 Steps of BCP Process

BCP involves more than planning for a move offsite after a disaster destroys a data centre. It also addresses how to keep an organisation's critical functions operating in the event of disruptions, both large and small. This broader perspective on contingency planning is based on the distribution of computer support throughout an organisation. Management of organisations are responsible for implementing BCP. IS Auditor is responsible for validating the required BCP processes are implemented and meet the organisation requirements of BCP. A brief overview of the BCP processes are explained below. The six steps in a BCP process are:

1. Identifying the mission- or business-critical functions
2. Identifying the resources that support the critical functions
3. Anticipating potential contingencies or disasters
4. Selecting contingency planning strategies
5. Implementing the contingency strategies
6. Testing and revising the strategy

3.2.1 Step 1: Identifying the mission or business-critical functions

Protecting the continuity of an organization's mission or business is very difficult if it is not clearly identified. Managers need to understand the organisation from a point of view that usually extends beyond the area they control. The definition of an organisation's critical mission or

business functions is often called a business plan. Since the development of a business plan will be used to support contingency planning, it is necessary not only to identify critical missions and businesses, but also to set priorities for them. A fully redundant capability for each function is prohibitively expensive for most organisations. In the event of a disaster, certain functions will not be performed. If appropriate priorities have been set (and approved by senior management), this could make the difference in the organisation's ability to survive a disaster.

3.2.2 Step 2: Identifying the resources that support critical functions

BCP has to address all the resources needed to perform a function, regardless whether they directly relate to a computer. The analysis of needed resources is to be conducted by those who understand how the function is performed and the dependencies of various resources on other resources and other critical relationships. This will allow an organisation to assign priorities to resources since not all elements of all resources are crucial to the critical functions. Some of the critical tasks and resources of BCP are explained below.

1. Human Resources

People are perhaps an organisation's most obvious resource. Some functions require the effort of specific individuals, some require specialized expertise, and some only require individuals who can be trained to perform a specific task. Within the information technology field, human resources include both operators (such as technicians or system programmers) and users (such as data entry clerks or information analysts).

2. Processing capability

Traditionally contingency planning has focused on processing power (i.e., if the data centre is down, how can applications dependent on it continue to be processed?). Although the need for data centre backup remains vital, today's other processing alternatives are also important. Local area networks (LANs), minicomputers, workstations, and personal computers in all forms of centralised and distributed processing may be performing critical tasks.

3. Automated applications and data

Computer systems run applications that process data. Without current electronic versions of both applications and data, computerised processing may not be possible. If the processing is being performed on alternate hardware, the applications must be compatible with the alternate hardware, operating systems and other software (including version and configuration), and numerous other technical factors. Because of the complexity, it is normally necessary to periodically verify compatibility.

4. Computer-based services

An organisation uses many different kinds of computer-based services to perform its functions. The two most important are normally communications services and information services. Communications can be further categorised as data and voice communications; however, in many organisations these are managed by the same service. Information services include any source of information outside of the organisation.

5. Physical infrastructure

For people to work effectively, they need a safe working environment and appropriate equipment and utilities. This can include office space, heating, cooling, venting, power, water, sewage, other utilities, desks, telephones, fax machines, personal computers, terminals, courier services, file cabinets, and many other items. In addition, computers also need space and utilities, such as electricity. Electronic and paper media used to store applications and data also have physical requirements.

6. Documents and papers

Many functions rely on vital records and various documents, papers, or forms. These records could be important because of a legal need (such as being able to produce a signed copy of a loan) or because they are the only record of the information. Records can be maintained on paper, microfiche, microfilm, magnetic media, or optical disk.

3.2.3 Step 3: Anticipating potential contingencies or disasters

Although it is impossible to think of all the things that can go wrong, the next step is to identify a likely range of problems. The development of scenarios will help an organisation develop a plan to address the wide range of things that can go wrong. Scenarios are to include small and large contingencies. While some general classes of contingency scenarios are obvious, imagination and creativity, as well as research, can point to other possible, but less obvious, contingencies. The contingency scenarios have to address each of the resources described above.

3.2.4 Step 4: Selecting contingency planning strategies

The next step is to plan how to recover needed resources. In evaluating alternatives, it is necessary to consider what controls are in place to prevent and minimise contingencies. Since no set of controls can cost-effectively prevent all contingencies, it is necessary to co-ordinate prevention and recovery efforts. A contingency planning strategy normally consists of three parts: emergency response, recovery, and resumption. Emergency response encompasses the initial actions taken to protect lives and limit damage. Recovery refers to the steps that are taken to continue support for critical functions. Resumption is the return to normal operations. The relationship between recovery and resumption is important. The longer it takes to resume normal operations, the longer the organisation will have to operate in the recovery mode.

3.2.5 Step 5: Implementing the contingency strategies

Once the contingency planning strategies have been selected, it is necessary to make appropriate preparations, document the strategies, and train employees. Many of these tasks are ongoing.

1. Implementation

Much preparation is needed to implement the strategies for protecting critical functions and their supporting resources. For example, one common preparation is to establish procedures for backing up files and applications. Another is to establish contracts and agreements, if the contingency strategy calls for them. Existing service contracts may need to be renegotiated to add contingency services. Another preparation may be to purchase equipment, especially to support a redundant capability.

2. Back up

Backing up data files and applications is a critical part of virtually every contingency plan. Backups are used, for example, to restore files after a personal computer virus corrupts the files or after a hurricane destroys a data processing centre.

3. Documentation

It is important to keep preparations, including documentation, up-to-date. Computer systems change rapidly and so should backup services and redundant equipment. Contracts and agreements may also need to reflect the changes. If additional equipment is needed, it must be maintained and periodically replaced when it is no longer dependable or no longer fits the organization's architecture.

4. Assigning responsibility

Preparation should also include formally designating people who are responsible for various tasks in the event of a contingency. These people are often referred to as the contingency response team. This team is often composed of people who were a part of the contingency planning team.

5. No. of BC Plans and responsibility

There are many important implementation issues for an organization. Two of the most important are firstly: How many plans should be developed and secondly: Who prepares each plan? Both of these questions revolve around the organisation's overall strategy for contingency planning. The answers should be documented in organisation policy and procedures. Some organizations have just one plan for the entire organisation, and others have a plan for every distinct computer system, application, or other resource. However, it is important to ensure co-ordination between various functional heads responsible for managing critical resources.

3.2.6 Step 6: Testing and Revising

A BC plan has to be tested periodically because there will undoubtedly be flaws in the plan and in its implementation. The plan will become dated as time passes and as the resources used to support critical functions change. Responsibility for keeping the plan updated has to be clearly defined in the BC Plan.

3.3 Audit and Regulatory requirements

Business Continuity Planning (BCP) refers to ability of organisations to recover from a disaster and continue operations with least impact. It is imperative that every organisation whether profit-oriented or service-oriented has a business continuity plan as relevant to the activities of the organisation. It is not enough that organisation has a BCP but it is also important to have an independent audit of BCP to confirm its adequacy and appropriateness to meet the needs of the organisation.

3.3.1 Role of IS Auditor in BCP Audit

In a BCP Audit, the IS auditor is expected to evaluate the processes of developing and maintaining documented, communicated, and tested plans for continuity of business operations and IS processing in the event of a disruption. The objective of BCP review is to assess the ability of the organisation to continue all critical operations during a contingency and recover from a disaster within the defined critical recover time period. IS Auditor is expected to identify residual risks which are not identified and provide recommendations to mitigate them. The plan of action for each type of expected contingency and its adequacy in meeting contingency requirements is also assessed in a BCP audit. BCP of an organisation is also to be reviewed to a limited extent for the assessment of an auditee organisation from the perspective of going concern.

3.3.2 Regulatory requirements

A business continuity plan audit should provide management an evaluation of the organisation's preparedness in the event of a major business disruption. It should identify issues that may limit interim business processing and restoration of same. It should also provide management with an independent assessment of the effectiveness of the business continuity plan and its alignment with subordinate continuity plans. The business continuity plan audit should be programmed to cover the applicable laws, standards and Frameworks etc. Understanding of the applicable regulatory requirements are essential while doing the audit of any BCP environment to ensure whether the information technology arrangement related to Business continuity and disaster recovery plans are in conformity with the applicable Laws and regulations. It is also necessary to understand whether the information technology related to BCP/DRP arrangements are supporting the business compliance with external laws and regulations. Hence before designing the audit scope and programmes all external compliance requirements are to be identified and external compliance requirements are adequately addressed. This can be ensured by adopting the following management practices as suggested by COBIT 5 Process MEA03 Monitor, Evaluate and Assess Compliance with External Requirements. COBIT stands for Control Objectives for Information and Related Technology. Given below are some relevant extracts from COBIT 5: Enabling process which are relevant and can be adapted for implementing or reviewing BCP processes of any organisation.

Using COBIT best practices for evaluating regulatory compliances

MEA03 Monitor, Evaluate and Assess Compliance with External Requirements

Process Scope

Evaluate that IT processes and IT-supported business processes are compliant with laws, regulations and contractual requirements. Obtain assurance that the requirements have been identified and complied with, and integrate IT compliance with overall organisation compliance.

Process Purpose

Ensure that the organisation is compliant with all applicable external requirements.

Management Practices

1. On a continuous basis, identify and monitor for changes in local and international laws, regulations and other external requirements that must be complied with from an IT perspective. This will be achieved by doing following activities:

- Assign responsibility for identifying and monitoring any changes of legal, regulatory and other external contractual requirements relevant to the use of IT resources and the processing of information within the business and IT operations of the organisation.
- Identify and assess all potential compliance requirements and the impact on IT activities in areas such as data flow, privacy, internal controls, financial reporting, industry-specific regulations, intellectual property, health and safety.
- Assess the impact of IT-related legal and regulatory requirements on third-party contracts related to IT operations, service providers and business trading partners.
- Obtain independent counsel, where appropriate, on changes to applicable laws, regulations and standards.
- Maintain an up-to-date log of all relevant legal, regulatory and contractual requirements, their impact and required actions.
- Maintain a harmonised and integrated overall register of external compliance requirements for the organisation.

2. Review and adjust policies, principles, standards, procedures and methodologies to ensure that legal, regulatory and contractual requirements are addressed and communicated. Consider industry standards, codes of good practice, and best practice guidance for adoption and adaptation. This can be achieved by doing following activities:
   - Regularly review and adjust policies, principles, standards, procedures and methodologies for their effectiveness in ensuring necessary compliance and addressing organisation risk using internal and external experts, as required.
   - Communicate new and changed requirements to all relevant personnel.
3. Confirm compliance of policies, principles, standards, procedures and methodologies with legal, regulatory and contractual requirements. This is ensured by adopting the following activities:
   - Regularly evaluate organisational policies, standards, procedures and methodologies in all functions of the organisation to ensure compliance with relevant legal and regulatory requirements in relation to the processing of information.
   - Address compliance gaps in policies, standards and procedures on a timely basis.
   - Periodically evaluate business and IT processes and activities to ensure adherence to applicable legal, regulatory and contractual requirements.
   - Regularly review for recurring patterns of compliance failures. Where necessary, improve policies, standards, procedures, methodologies, and associated processes and activities.
4. Obtain and report assurance of compliance and adherence with policies, principles, standards, procedures and methodologies. Confirm that corrective actions to address compliance gaps are closed in a timely manner. To ensure this management practice the following activities are to be ensured:

- Obtain regular confirmation of compliance with internal policies from business and IT process owners and unit heads.
- Perform regular (and, where appropriate, independent) internal and external reviews to assess levels of compliance.
- If required, obtain assertions from third-party IT service providers on levels of their compliance with applicable laws and regulations.
- If required, obtain assertions from business partners on levels of their compliance with applicable laws and regulations as they relate to intercompany electronic transactions.
- Monitor and report on non-compliance issues and, where necessary, investigate the root cause.
- Integrate reporting on legal, regulatory and contractual requirements at an organisation wide level, involving all business units.

3.3.3 Regulatory compliances of BCP

Regulatory requirements play an important role in outlining the need for BCP for organisations which provide critical services. These regulations also provide generic guidelines for implementing BCP. Some of the sample laws and regulations that are applicable are given here:

Basel Committee on E-Banking

The Basel Committee on E-Banking outlines the principles for electronic banking as; Banks should have effective capacity, business continuity and contingency planning processes to help ensure the availability of e-banking systems and services". The Committee underlines that banks should also ensure that periodic independent internal and/or external audits are conducted about business continuity and contingency planning. These requirements are spelt out in Appendix VI relating to "Sound Capacity, Business Continuity and Contingency Planning Practices for E-Banking":

Indian legislations

There are various Indian legislations such as the Information Technology Act, Indian Income tax Act, Central Sales Tax act, State VAT Acts, Services Tax Act, Central Excise Act etc. which require data retention for specific number of years. Organisations which have to comply with these requirements have to ensure that they have a proper business continuity plan which meets these requirements. The Reserve Bank of India provides regular guidelines to financial institutions covering various aspects of IT deployment. These guidelines cover business continuity and disaster recovery procedures for various types of business operations which are dependent on IT environment.

Bank Audit

The Long Form Audit Report in the case of statutory audit of banks contains two key points relating to business continuity and disaster recovery which need to be evaluated and commented by the statutory auditor.

- Whether regular back ups of accounts and off-site storage are maintained as per the guidelines of the controlling authorities of the bank?
- Whether adequate contingency and disaster recovery plans are in place for loss/encryption of data?

The first point may be irrelevant in case of audit of branches where core banking solution is implemented. However, a general review of the contingency and disaster recovery plans has to be made by auditor and required comments provided. In case of internal audit or concurrent audit of banks, there are specific areas of BCP which need to be reviewed by the auditors.

3.4 Using best practices and frameworks for BCP

3.4.1 COBIT 5

COBIT 5 is a framework of business governance. It provides a set of best practices for Governance and management of Organisation IT. Best practices pertaining to BCM can be selected and adapted as required. Below is an extract of management practices and activities from COBIT which is applicable to BCP.

DSS04: Manage continuity

Process Scope

Establish and maintain a plan to enable the business and IT to respond to incidents and disruptions in order to continue operation of critical business processes and required IT services and maintain availability of information at a level acceptable to the organisation.

Process Purpose

Continue critical business operations and maintain availability of information at a level acceptable to the organisation in the event of a significant disruption.

Management Practices and activities

1. **Define the business continuity policy, objectives and scope:** Define business continuity policy and scope aligned with organisation and stakeholder objectives.
    - Identify internal and outsourced business processes and service activities that are critical to the organisation operations or necessary to meet legal and/or contractual obligations.
    - Identify key stakeholders and roles and responsibilities for defining and agreeing on continuity policy and scope.
    - Define and document the agreed-on minimum policy objectives and scope for business continuity and embed the need for continuity planning in the organisation culture.
    - Identify essential supporting business processes and related IT Services.
2. **Maintain a continuity strategy:** Evaluate business continuity management options and choose a cost-effective and viable continuity strategy that will ensure organisation recovery and continuity in the face of a disaster or other major incident or disruption.

- Identify potential scenarios likely to give rise to events that could significant disruptive incidents.
- Conduct a business impact analysis to evaluate the impact overtime of a disruption to critical business functions and the effect that a disruption would have on them.
- Establish the minimum time required to recover a business process and supporting IT based on an acceptable length interruption and maximum tolerable outrage.
- Assess the likelihood of threats that could cause loss of business continuity and identify measures that will reduce the likelihood and impact through improved prevention and increased resilience.
- Analyse continuity requirements to identify the possible strategic business and technical options.
- Determine the conditions and owners of key decisions that will cause the continuity plans to be invoked.
- Identify resource requirements and costs for each strategic technical option and make strategic recommendations.
- Obtain executive business approval for selected strategic options.

3. **Develop and implement a business continuity response :** Develop a business continuity plan (BCP) based on the strategy that documents the procedures and information in readiness for use in an incident to enable the organisation to continue its critical activities.
   - Define the incident response actions and communications to be taken in the event of disruption. Define related roles and responsibilities, including accountability for policy and implementation.
   - Develop and maintain operational BCPs containing the procedures to be followed to enable continued operation of critical business processes and/or temporary processing arrangements, including links to plans of outsourced service providers.
   - Ensure that key suppliers and outsource partners have effective continuity plans in place. Obtain audited evidence as required.
   - Define the conditions and recovery procedures that would enable resumption of business processing, including updating and reconciliation of information databases to preserve information integrity.
   - Define and document the resources required to support the continuity and recovery procedures, considering people, facilities and IT infrastructure.
   - Define and document the information backup requirements required to support the plans, including plans and paper documents as well as data files, and consider the need for security and off-site storage.
   - Determine required skills for individuals involved in executing the plan and procedures.
   - Distribute the plans and supporting documentation securely to appropriately authorise interested parties and make sure they are accessible under all disaster scenarios.

4. **Exercise, test and review the BCP:** Test the continuity arrangements on a regular basis to exercise the recovery plans against predetermined outcomes and to allow innovative solutions to be developed and help to verify over time that the plan will work as anticipated.
    - Define objectives for exercising and testing the business, technical, logistical, administrative, procedural and operational systems of the plan to verify completeness of the BCP in meeting business risk.
    - Define and agree on with stakeholders exercises that are realistic, validate continuity procedures, and include roles and responsibilities and data retention arrangements that cause minimum disruption to business processes.
    - Assign roles and responsibilities for performing continuity plan exercises and tests.
    - Schedule exercises and test activities as defined in the continuity plan.
    - Conduct a post-exercise debriefing and analysis to consider the achievement.
    - Develop recommendations for improving the current continuity plan based on the results of the review.
5. **Review, maintain and improve the continuity plan:** Conduct a management review of the continuity capability at regular intervals to ensure its continued suitability, adequacy and effectiveness. Manage changes to the plan in accordance with the change control process to ensure that the continuity plan is kept up-to-date and continually reflects actual business requirements.
    - Review the continuity plan and capability on a regular basis against any assumptions made and current business operational and strategic objectives.
    - Consider whether a revised business impact assessment may be required, depending on the nature of the change.
    - Recommend and communicate changes in policy, plans, procedures, infrastructure, and roles and responsibilities for management approval and processing via the change management process.
    - Review the continuity plan on a regular basis to consider the impact of new or major changes to: organisation, business processes, outsourcing arrangements, technologies, infrastructure, operating systems and application systems.
6. **Conduct continuity plan training :** Provide all concerned internal and external parties with regular training sessions regarding the procedures and their roles and responsibilities in case of disruption.
    - Define and maintain training requirements and plans for those performing continuity planning, impact assessments, risk assessments, media communication and incident response. Ensure that the training plans consider frequency of training and training delivery mechanisms.
    - Develop competencies based on practical training including participation in exercises and tests.
    - Monitor skills and competencies based on the exercise and test results.

7. **Manage backup arrangements:** Maintain availability of business critical information.
    - Backup systems, applications, data and documentation according to a defined schedule, considering:
        - Frequency (monthly, weekly, daily, etc.)
        - Mode of backup (e.g., disk mirroring for real-time backups vs. DVD-ROM for long-term retention)
        - Type of backup (e.g., full vs. incremental)
        - Type of media
        - Automated online backups
        - Data types (e.g., voice, optical)
        - Creation of logs
        - Critical end-user computing data (e.g., spreadsheets)
        - Physical and logical location of data sources
        - Security and access rights
        - Encryption
    - Ensure that systems, applications, data and documentation maintained or processed by third parties are adequately backed up or otherwise secured. Consider requiring return of backups from third parties. Consider escrow or deposit arrangements.
    - Define requirements for on-site and off-site storage of backup data that meet the business requirements. Consider the accessibility required to back up data.
    - Roll out BCP awareness and training.
    - Periodically test and refresh archived and backup data.
8. **Conduct post-resumption review:** Assess the adequacy of the BCP following the successful resumption of business processes and services after a disruption.
    - Assess adherence to the documented BCP.
    - Determine the effectiveness of the plan, continuity capabilities, roles and responsibilities, skills and competencies, resilience to the incident, technical infrastructure, and organisational structures and relationships.
    - Identify weaknesses or omissions in the plan and capabilities and make recommendations for improvement.
    - Obtain management approval for any changes to the plan and apply via the organisation change control process.

BAI04: Manage Availability and Capacity

Process Scope

Balance current and future needs for availability, performance and capacity with cost-effective service provision. Include assessment of current capabilities, forecasting of future needs based

on business requirements, analysis of business impacts, and assessment of risk to plan and implement actions to meet the identified requirements.

Process Purpose

Maintain service availability, efficient management of resources, and optimisation of system performance through prediction of future performance and capacity requirements.

Management Practices and activities

1. **Assess current availability, performance and capacity and create a baseline:** Assess availability, performance and capacity of services and resources to ensure that cost-justifiable capacity and performance are available to support business needs and deliver against SLAs. Create availability, performance and capacity baselines for future comparison.
    - Consider the following (current and forecasted) in the assessment of availability, performance and capacity of services and resources: customer requirements, business priorities, business objectives, budget impact, resource utilisation, IT capabilities and industry trends.
    - Monitor actual performance and capacity usage against defined thresholds, supported where necessary with automated software.
    - Identify and follow up on all incidents caused by inadequate performance or capacity.
    - Regularly evaluate the current levels of performance for all processing levels (business demand, service capacity and resource capacity) by comparing them against trends and SLAs, taking into account changes in the environment.
2. **Assess business impact:** Identify important services to the organisation, map services and resources to business processes, and identify business dependencies. Ensure that the impact of unavailable resources is fully agreed on and accepted by the customer. Ensure that, for vital business functions, the SLA availability requirements can be satisfied.
    - Identify only those solutions or services that are critical in the availability and capacity management process.
    - Map the selected solutions or services to application(s) and infrastructure (IT and facility) on which they depend to enable a focus on critical resources for availability planning.
    - Collect data on availability patterns from logs of past failures and performance monitoring. Use modelling tools that help predict failures based on past usage trends and management expectations of new environment or user conditions.
    - Create scenarios based on the collected data, describing future availability situations to illustrate a variety of potential capacity levels needed to achieve the availability performance objective.
    - Determine the likelihood that the availability performance objective will not be achieved based on the scenarios.
    - Determine the impact of the scenarios on the business performance measures (e.g., revenue, profit, customer services). Engage the business line, functional (especially finance) and regional leaders to understand their evaluation of impact.

- Ensure that business process owners fully understand and agree to the results of this analysis. From the business owners, obtain a list of unacceptable risk scenarios that require a response to reduce risk to acceptable levels.

3. **Plan for new or changed service requirements:** Plan and prioritise availability, performance and capacity implications of changing business needs and service requirements.
   - Review availability and capacity implications of service trend analysis.
   - Identify availability and capacity implications of changing business needs and improvement opportunities. Use modelling techniques to validate availability, performance and capacity plans.
   - Prioritise needed improvements and create cost-justifiable availability and capacity plans.
   - Adjust the performance and capacity plans and SLAs based on realistic, new, proposed and/or projected business processes and supporting services, applications and infrastructure changes as well as reviews of actual performance and capacity usage, including workload levels.
   - Ensure that management performs comparisons of actual demand on resources with forecasted supply and demand to evaluate current forecasting techniques and make improvements where possible.
4. **Monitor and review availability and capacity:** Monitor, measure, analyses, report and review availability, performance and capacity. Identify deviations from established baselines. Review trend analysis reports identifying any significant issues and variances, initiating actions where necessary, and ensuring that all outstanding issues are followed up.
   - Establish a process for gathering data to provide management with monitoring and reporting information for availability, performance and capacity workload of all information-related resources.
   - Provide regular reporting of the results in an appropriate form for review by IT and business management and communication to organisation management.
   - Integrate monitoring and reporting activities in the iterative capacity management activities (monitoring, analysis, tuning and implementations).
   - Provide capacity reports to the budgeting processes.
5. **Investigate and address availability, performance and capacity issues:** Address deviations by investigating and resolving identified availability, performance and capacity issues.
   - Obtain guidance from vendor product manuals to ensure an appropriate level of performance availability for peak processing and workloads.
   - Identify performance and capacity gaps based on monitoring current and forecasted performance. Use the known availability, continuity and recovery specifications to classify resources and allow prioritisation.
   - Define corrective actions (e.g., shifting workload, prioritising tasks or adding resources, when performance and capacity issues are identified).

- Integrate required corrective actions into the appropriate planning and change management processes.
- Define an escalation procedure for swift resolution in case of emergency capacity and performance problems.

For more information, please www.isaca.org/cobit.

3.4.2 ISO 22301: Standard on Business Continuity Management

ISO 22301 specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to prepare for, respond to and recover from disruptive events when they arise. The requirements specified in ISO 22301 are generic and intended to be applicable to all organisations (or parts thereof), regardless of type, size and nature of the organisation. The extent of application of these requirements depends on the organisation's operating environment and complexity. Following the new structure of the ISO Guide 83, ISO 22301 is organised into the following main clauses:

- Clause 4: Context of the organisation
- Clause 5: Leadership
- Clause 6: Planning
- Clause 7: Support
- Clause 8: Operation
- Clause 9: Performance evaluation
- Clause 10: Improvement

For more information, please visited www.iso.org.

3.4.3 ITIL

Information Technology Infrastructure Library (ITIL), a UK body, is a collection of best practices in IT service management, consisting of a series of books giving guidance on the provision of quality IT services. ITIL is drawn from the public and private sectors internationally, supported by a comprehensive qualification scheme and accredited training organisations. ITIL is the most widely adopted approach for IT Service Management in the world. It provides a practical, no-nonsense framework for identifying, planning, delivering and supporting IT services to the business. It includes descriptions of best practice in information security management as well as other related disciplines. For more information, please visit: www.itil-officialsite.com.

3.4.4 SSAE 16

Statement on Standards for Attestation Engagements (SSAE) No. 16, known as SSAE 16, has been put forth by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA). SSAE 16 is an "attest" standard that closely mirrors its international "assurance" equivalent, ISAE 3402, which was issued by the International Auditing and Assurance Standards Board (IAASB), a standard-setting board of the International Federation of Accountants (IFAC). SSAE 16 is issued by AICPA. It is generally applicable when an auditor (called the "user auditor") is auditing the financial statements of an entity ("user organisation") that obtains services

from another organisation ("service organisation"). The service organisations that provide such services could be application service providers, bank trust departments, claims processing centres, Internet data centres, or other data processing service bureaus.. For more information, please visit: www.ssae16.org

3.4.5 Audit Tools and Techniques

The objective of BCP audit is to provide assurance to management on adequacy of BCP process and DRP procedures, identify control gaps, ensure regulatory compliance and ensure business process owners are accountable for their plans and testing. The best audit tool and technique is a periodic simulation of a disaster. Other audit techniques would include observations, interviews, checklists, inquiries, meetings, questionnaires and documentation reviews. These tools and methods may be categorized as explained here.

i. **Automated Tools:** Automated tools make it possible to review large computer systems for a variety of flaws in a short time period. They can be used to find threats and vulnerabilities such as weak access controls, weak passwords, lack of integrity of the system software, etc.

ii. **Internal Control Auditing:** This includes inquiry, observation and testing. The process can detect illegal acts, errors, irregularities or lack of compliance of laws and regulations.

iii. **Disaster and Security Checklists:** A checklist can be used against which the system can be audited. The checklist should be based upon disaster recovery policies and practices, which form the baseline. Checklists can also be used to verify changes to the system from contingency point of view.

iv. **Penetration Testing:** Penetration testing can be used to locate vulnerabilities in the network.

3.4.6 Service Level Agreement

A service level agreement is an agreement between the organisation and the customer. The SLA details are the services(s) to be provided. The IT organisation could be an internal IT department or an external IT service provider, and the customer is the business. The business may acquire IT services from an internal IT organisation, such as e-mail services, an intranet, an organisation resource planning (ERP) system, etc. the business may acquire IT services from an external IT service provider, such as internet connectivity, hosting of a public website. The SLA describes the services in non technical terms, from the viewpoint of the customer.

During the term of the agreement, it serves as the standard for measuring and adjusting the services. Service levels are often defined to include hardware and software performance targets (such as user response time and hardware availability) but can also include a wide range of other performance measures. Such measures might include financial performance measures (such as year-to-year incremental cost reduction), human relationship measures (such as resource planning, staff turnover, development and training) or risk management measures (compliance with control objectives).

The IS auditor should be aware of the different types of measures available and should ensure that they are comprehensive and include risk, security and control measures as well as security and control measures as well as efficiency and effectiveness measures.

Where the functions of a BCP are outsourced, the IS auditor should determine how management gains assurance that the controls at the third party are properly designed and operating effectively. Several techniques can be used by management, including questionnaires, onsite visits or an independent third-party assurance report such as an SSAE 16 SOC 1 report or SOC 2 or SOC 3 report.

3.5 Services that can be provided by an IS Auditor in BCM

1. Management Consultancy Services in providing guidance in drafting of a BCP/DRP. CAs can provide insight to the organisation on the development of a BCP/DRP. Appropriate guidance in drafting a BCP such as scoping of the BCP as per the policy etc. Development of a BCP Manual.
2. Management Consultancy Services in designing and implementing a BCP/DRP. CAs can provide guidance in the actual design of the BCP that is relevant to the organisation's nature and size. They can assist the management in implementing the BCP in the organisation. They can design the phases for implementation of the BCP and thus ensure correct and effective implementation of the BCP in the organisation.
3. Designing Test Plans and Conducting Tests of the BCP/DRP. CAs can design plans that can be used by the management for regular testing of the BCP. He can also evaluate the tests that have been conducted by the management.
4. Consultancy Services in revising and updating the BCP/DRP. Maintenance of the BCP is a periodic process. Technologies evolve and the Business Environment often changes and hence it is necessary to revise and update the BCP.
5. Conducting Pre Implementation Audit, Post Implementation Audit, General Audit of the BCP/DRP.

   A Chartered Accountant can provide assurance whether the BCP would suffice to the organisation.
6. Consultancy Services in Risk Assessment and Business Impact Analysis. Conducting a proper Business Impact Analysis and assessing the risks that are present in the organisation's environment is really crucial for the correct development of the BCP/DRP. CAs can help in the development stages by conducting BIA and Risk Assessment for the organisation.
7. CAs can be involved in any/all areas of BCP implementation or review. These areas could be pertaining to:
   a. Risk Assessment
   b. Business Impact Assessment
   c. Disaster Recovery Strategy Selection
   d. Business Continuity Plan Development
   e. Fast-track Business Continuity Development
   f. BCP / DRP Audit, Review and Health-check Services
   g. Development and Management of BCP / DRP Exercises and Rehearsals
   h. Media Management for Crisis Scenarios
   i. Business Continuity Training

3.6 Summary

A BCP is not merely about information Technology Assets but is also about people reactions in case of a crisis. In a crisis, people have to assume responsibilities that are different from their normal day to day tasks. This requires a series of co-ordinated actions on the part of the personnel involved. A BCP is rarely a standalone document. It is, usually, part of a set of documents... There may be a separate plan, the Cyber Incident Response Plan, to take care of threats like computer viruses and network intrusions. An Occupant Emergency Plan (OEP) may be in use for the evacuation of premises during a fire or medical emergencies. Insurance is yet another tool that supplements BCP. Monetary losses can be minimized by transferring certain risks to an insurance company on the payment of a premium. A BCP that exists on paper without being tested serves no useful purpose. The worst possible way to "test" is to see whether it works during a real disaster. Ideally, while framing the objectives of the BCP, the organisation spells out the "acceptance criteria", that is, the tests that will validate the BCP. Testing a BCP can be a complex undertaking as many personnel will have to carry out the tests even while continuing with normal operations.

After the completion of Chapter 3, we can summarise the broad coverage as follows:

- IS Auditor has to understand BCP processes and key activities for each of the key processes. This chapter has provided an overview of the BCP processes.
- Regulations such as the Sarbanes Oxley Act, HIPAA, and BASEL 2 make it mandatory for an organisation to have Business Continuity Management. Standards such as ISO 22301, 27000 etc. and Frameworks such as COBIT, ITIL lays down the steps that could be followed by the management of the organisation to have efficient Business Continuity Management Practices.
- Audit Process that are to be followed by an IS Auditor. A control is placed always against an identified risk by the management. It is essential for an IS Auditor to verify the controls that have been put in place by the management for adequacy and existence. IS auditor has to follow the standard auditing procedures and guidance notes (if any) issued by the governing bodies (Like ICAI in case of Chartered Accountants, ISACA in case of certified information system auditors etc.) while discharging their duties.

3.7 References

www.icai.org

www.isaca.org

www.csoonline.com

www.thebci.org

www.aicpa.org

www.iso.org

www.bsigroup.org

3.8 Questions

1. An IS auditor reviewing an organisation's information systems disaster recovery plan should verify that it is:
   A. Tested every 1 month.
   B. Regularly reviewed and updated.
   C. Approved by the chief executive officer
   D. Approved by the top management
2. Which of the following would an IS auditor consider to be the MOST important to review when conducting a business continuity audit?
   A. A hot site is contracted for and available when needed.
   B. A business continuity manual is available and current.
   C. Insurance coverage is sufficient
   D. Media backups are performed on a timely basis and stored off-site.
3. Which of the following findings would an IS auditor be MOST concerned about when performing an audit of backup and recovery and the offsite storage vault?
   A. There are three individuals with a key to enter the area
   B. Paper documents are also stored in the offsite vault
   C. Data files, which are stored in the vault, are synchronised
   D. The offsite vault is located in a separate facility
4. A company performs full back-up of data and programmes on a regular basis. The primary purpose of this practice is to:
   A. Maintain data integrity in the applications.
   B. Restore application processing after a disruption.
   C. Prevent unauthorised changes to programmes and data.
   D. Ensure recovery of data processing in case of a disaster.
5. Which of the following procedures would an IS auditor perform to BEST determine whether adequate recovery/restart procedures exist?
   A. Reviewing programme code
   B. Reviewing operations documentation
   C. Turning off the UPS, then the power
   D. Reviewing programme documentation

6. An IS auditor performing a review of the back-up processing facilities would be MOST concerned that:

   A. Adequate fire insurance exists.

   B. Regular hardware maintenance is performed.

   C. Offsite storage of transaction and master files exists.

   D. Backup processing facilities are fully tested.

7. Which of the following offsite information processing facility conditions would cause an IS auditor the GREATEST concern?

   A. Company name is clearly visible on the facility.

   B. The facility is located outside city limits from the originating city.

   C. The facility does not have any windows.

   D. The facility entrance is located in the back of the building rather than the front.

8. Which of the following methods of results analysis, during the testing of the business continuity plan (BCP), provides the BEST assurance that the plan is workable?

   A. Quantitatively measuring the results of the test

   B. Measurement of accuracy

   C. Elapsed time for completion of prescribed tasks

   D. Evaluation of the observed test results

9. An IS auditor conducting a review of disaster recovery plan (DRP) at a financial processing organisation has noticed that existing DRP was compiled two years ago by a systems analystusing information from operations department. The plan was presented to CEO for approval but it is not yet approved. The plan has never been updated, tested or circulated to key management and staff, though interviews show that each would know what action to take for their area in the event of a disruptive incident. The IS auditor's report should recommend:

   A. The deputy CEO be censured for his failure to approve the plan.

   B. A board of senior managers be set up to review the existing plan.

   C. The existing plan be approved and circulated to all key management and staff.

   D. An experienced manager co-ordinates the creation of a new plan or revised plan within a defined time limit.

10. Which of the following would be of MOST concern for an IS auditor reviewing back-up facilities?

    A. Adequate fire insurance exists.

    B. Regular hardware maintenance is performed.

    C. Offsite storage of transaction and master files exists.

    D. Backup processing facilities are fully tested.

3.9 Answers and Explanations

1. B. The plan must be reviewed at appropriate intervals, depending upon the nature of the business and the rate of change of systems and personnel, otherwise it may quickly become out of date and may no longer be effective (for example, hardware or software changes in the live processing environment are not reflected in the plan). The plan must be subjected to regular testing, but the period between tests will depend on nature of the organisation and relative importance of IS. Three months or even annually may be appropriate in different circumstances. Although the disaster recovery plan should receive the approval of senior management, it need not be the CEO if another executive officer is equally, or more appropriate. For a purely IS-related plan, the executive responsible for technology may have approved the plan. the IS disaster recovery plan will usually be a technical document and relevant to IS and communications staff only.
2. D. Without data to process, all other components of the recovery effort are in vain. Even in the absence of a plan, recovery efforts of any type would not be practical without data to process.
3. C. More than one person would need to have a key to the vault and location of the vault is important, but not as important as the files being synchronised. Choice A is incorrect because more than one person would typically need to have a key to the vault to ensure that individuals responsible for the offsite vault can take vacations and rotate duties. Choice B is not correct because the IS auditor would not be concerned whether paper documents are stored in the offsite vault. In fact, paper documents such as procedural documents and a copy of the contingency plan would most likely be stored in the offsite vault.
4. B. Back-up procedures are designed to restore programmes and data to a previous state prior to computer or system disruption. These backup procedures merely copy data and do not test or validate integrity. Back-up procedures will also not prevent changes to programme and data. On the contrary, changes will simply be copied. Although backup procedures can ease the recovery process following a disaster, they are not sufficient in themselves.
5. B. Operations documentation should contain recovery/restart procedures so that operations can return to normal processing in a timely manner. Turning off the UPS and then turning off the power might create a situation for recovery and restart, but the negative effect on operations would prove this method to be undesirable. The review of programme code and documentation generally does not provide evidence regarding recovery/restart procedures.
6. C. Adequate fire insurance and fully tested backup processing facilities are important elements for recovery, but without the offsite storage of transaction and master files, it is generally impossible to recover. Regular hardware maintenance does not relate to recovery.
7. A. The offsite facility should not be easily identified from the outside. Signs identifying the company and the contents of the facility should not be present. This is to prevent intentional sabotage of the offsite facility should the destruction of the originating site be from malicious attack. The offsite facility should not be subject to the same natural

disaster that affected the originating site. The offsite facility must also be secured and controlled just as the originating site. This includes adequate physical access controls such as locked doors, no windows and human surveillance.

8. A. Quantitatively measuring the results of the test involves a generic statement measuring all the activities performed during BCP, which gives the best assurance of an effective plan. Although choices B and C are also quantitative, they relate to specific areas or an analysis of results from one viewpoint, namely the accuracy of the results and the elapsed time.

9. D. The primary concern is to establish a workable disaster recovery plan which reflects current processing volumes to protect the organisation from any disruptive incident. Censuring the deputy CEO will not achieve this, and is generally not within the scope of an IS Auditor to recommend anyway. Setting up a board to review the plan, which is two years out of date, may achieve an updated plan, but is not likely to be a speedy operation and issuing the existing plan would be folly without first ensuring that it is workable. The best way to achieve a disaster recovery plan in a short timescale is to make an experienced manager responsible for co-ordinating the knowledge of other managers, as established by the audit interviews, into a single, formal document within a defined time limit.

10. C Adequate fire insurance and fully tested backup processing facilities are important elements for recovery, but without the offsite storage of transaction and master files, it is generally impossible to recover. Regular hardware maintenance does not relate to recovery.

SECTION 2: APPENDIX
CHECKLISTS AND CONTROL MATRIX

Appendix 1: Checklist for a Business Continuity Plan and Audit

Process Objectives:

- To seamlessly recover from the disaster situation.
- To reduce the impact of the damage of the assets, in turn reducing the data loss.
- To assure compliances
- To sustain operations so that customer service and corporate image can be maintained.

Using this Checklist

This checklist is to be used by the IS Auditor who is conducting the BCP Audit. This checklist covers the entire BCP Process but it has to be customized as per the specific needs of the assignment. An IS Auditor can use this checklist as a basis for recording observations and for collecting evidences for the Audit engagement. This is checklist is an illustrative example as to how an IS Auditor could conduct a BCM Audit at an organisation. It can be taken as a base for conducting such audit engagements.

Sl. No	Checkpoints/Particulars
Policy and Procedure	
1.	Is business continuity plan documented and implemented?
2.	Whether the scope and objectives of a BCP are clearly defined in the policy document? (Scope to cover all critical activities of business. Objectives should clearly spell out outcomes of the BCP)
3.	Whether there exist any exceptions to the scope of BCP i.e. in terms of location or any specific area, and whether the management has justifications for exclusion of the same.
4.	What is the time limit for such exclusion and what is the current strategy of covering such exclusions
5.	Are the policy and procedure documents approved by the Top Management?
6.	(Verify sign off on policy and procedure documents and budget allocations made by the management for a BCP) Does the business continuity plan ensure the resumption of IS operations during major information system failures? (Verify that the IS disaster recovery plan is in line with strategies, goals and objectives of corporate business continuity plan).
7.	Are users involved in the preparation of business continuity plan? (Managerial, operational, administrative and technical experts should be involved in the preparation of the BCP and DRP).

Sl. No	Checkpoints/Particulars
8.	Does the policy and procedure documents include the following List of critical information assets. List of vendor for service level agreements. Current and future business operations. Identification of potential threats and vulnerabilities. Business impact analysis. Involvement of technical and operational expert in preparation of BCP and Disaster recovery plans. Recovery procedure to minimise losses and interruptions in business operations. Disaster recovery teams. Training and test drills. Compliance with statutory and regulatory requirements
9.	Are the BCP policy and procedures circulated to all concerned? (Verify availability and circulation of the BCP & DRP to all concerned, including onsite and offsite storage).
10.	Is the business continuity plan updated and reviewed regularly? (Verify minutes of meeting where policy and procedures are reviewed. Verify amendments made to the policy and procedure documents due to the change in business environment).
Risk Assessment	
1.	Has the management identified potential threats/vulnerabilities to business operations? (Verify the business environment study report. Risk Assessment Report?)
2.	Are the risks evaluated by the Management? (Verify the probability or occurrence of the threat/vulnerability review carried out by the management).
3.	Has the organisation selected the appropriate method for risk evaluation?
4.	Has the organisation carried out the assessment of internal controls? (Verify the internal controls mitigating the risk).
5.	Has the organisation taken an appropriate decision on the risks identified? (Verify the decision-making on the options–accepted, reduced, avoided or transferred – for the risks identified).
6.	Are the risk assessment carried out at regular interval? (Verify the review frequency.)
Business Impact Analysis	
1.	Does the organisation carry out business impact analysis (BIA) for business operations?
2.	Has the organisation identified a BIA team?
3.	Are RTO and RPO defined by the management?
4.	Whether the SDO has been defined based upon RTO & RPO

Sl. No	Checkpoints/Particulars
5.	Whether the organisation has measured BIA? (Impact of risks on business operations can be measured in the form of business loss, loss of goodwill etc.)
6.	Is the business impact analysis carried out at a regular interval?
Development and Implementation of the BCP and DRP	
1.	Has the organisation prioritised recovery of interrupted business operations? (Prioritisation of activities is based on RTO and RPO)
2.	Has the organisation identified the various BCP and DRP Teams? (Verify employees are identified, informed and trained to take an action in the event of disaster).
3.	Are the responsibilities for each team documented? (Verify the roles and responsibilities assigned to employees for actions to be taken in the event of incident/disaster)
4.	Does the BCP document(s) include the following? Scope and objective. Roles and responsibilities of BCP and DRP Teams. Incident declaration. Contact list. Evacuation and stay-in procedure. Activity priorities. Human resource and welfare procedure. Escalation procedures. Procedure for resumption of business activities. Media communication. Legal and statutory requirements. Backup and restore procedures. Offsite operating procedures
5.	Are the copies of up-to-date BCP Documents stored offsite?
6.	Does the offsite facility have the adequate security requirements? (Verify the logical access, physical access and environmental control of the offsite).
7.	Does the BCP include training to employees? (Verify the evidences of training given).
8.	Whether the organisation has an adequate media and document backup and restoration procedures? (Verify the backup and restoration schedules adopted by the organisation)
9.	Are logs for backup and restoration maintained and reviewed? (Verify the logs maintained and review of the same by an independent person).
10.	Whether the media library has an adequate access control? (Verify the physical and logical access controls to the media library).
11.	Are the BCP and DRP communicated to all the concerned? (Verify availability and circulation of BCP & DRP to all concerned, including Onsite and offsite storage).

Sl. No	Checkpoints/Particulars
Maintenance of BCP and DRP	
1.	Whether the business continuity plan is tested at regular interval?
2.	Has the organisation reviewed the gap analysis of testing results? (Review process that includes a comparison of test results to the planned results).
3.	How has the organisation decided to reduce the gaps identified, what is the time limit set for addressing the same?
4.	Has the organisation got a testing plan? (Verify copy of test plan and updates).
5.	Are test drills conducted at appropriate intervals?
6.	Do organisation documents and analyses have testing results? (Verify the corrective copies of test results and analysis of the report).
7.	Has the organisation prepared action points to rectify the testing results? (Verify the corrective action plan for all problems encountered during the test drill).
8.	Does the organisation carry out retesting activity for action points? (Verify the evidences of retesting activities).
9.	Does the organisation review the BCP and DRP at regular intervals?
10.	Whether a review of the BCP includes following? BCP policy and procedure Scope and exclusion of BCP Inventory of IS assets Validating assumption made while risk assessment and preparation of BCP and DRP Risk assessment Business impact analysis Back up of system and data Training to employees Test drills

Appendix 2: Risk control matrix and audit guidelines for disaster recovery and Business Resumption Plan

The risk control matrix can be used by IS Auditors for identifying the relevant risks, implemented controls and steps to audit specific areas. This is a sample risk control matrix which can be adapted as required. The list of risks provides the key areas which are generally applicable for organisations. The relevant controls mitigate the risks.

Risk	Control	Audit Guidelines/Procedure
Non Existence of a Disaster Recovery/Business resumption Plan/improper planning methodologies used to create a DR/BCP could lead to a failure in resumption of critical business function.	The organisation should take steps in formulating a Business Continuity Policy. The policy should contain details regarding the methodologies used in formulating a DRP/BCP. Periodic.	• Identification and prioritisation of the activities which are essential to continue functioning. • The plan is based upon a business impact analysis that considers the impact of the loss of essential functions. • Operations managers and key employees participated in the development of the plan. • The plan identifies the resources that will likely be needed for recovery and the location of their availability. • The plan is simple and easily understood so that it will be effective when it is needed. • The plan is realistic in its assumptions.
Insufficient Backup processes could lead to data not being backed up correctly and restoration of data would not be possible. Backups without data pertaining to the software environment would lead to	Processes should include periodic backup of data which also involves storing data of the software those are dependent to render the files. Backups should be followed periodically and in the manner	• Determine if information backup procedures are sufficient to allow for recovery of critical data. • Determine if copies of the plan are safeguarded by off-site storage.

Risk	Control	Audit Guidelines/Procedure
data being restored but not possible to render such retrieved data due to lack of software.	prescribed in the Business Continuity Policy and signoffs should be obtained along with notification from the backup utility.	• Review information backup procedures in general. The availability of backup data could be critical in minimising the time needed for recovery. • Determine if the disaster recovery/ business re-sumption plan covers procedures for disaster declaration, general shut-down and migration of operations to the backup facility.
Insufficient testing of the BCP could lead to difficulties at the time of actual disaster.	Testing and revisions should be a part of the Policy. Test Plans drafted should be executed and reports regarding the tests should be maintained.	• Determine if a test plan exists and to what extent the disaster recovery/ business resumption plan has been tested. • Determine if a testing schedule exists and is adequate (at least annually). Verify the date of the last test. Determine if weaknesses identified in the last tests were corrected.
Lack of Required Resources those are essential to execute a DRP/BCP will lead to a failed execution.	The required resources should be procured and preserved. The resources needs to be reviewed periodically and changed as there could be wear and tear due to efflux of time. The required resources should be in accordance to the BCP/DRP.	• Determine if resources have been made available to maintain the disaster recovery/business resumption plan and keep it current. • Have resources been allocated to prevent the disaster recovery/ business resumption plan from becoming outdated and ineffective?
BCP/DRP without correct review of the existing plans, Business Impact Analysis and Risk Assessment would	BCP/DRP which has been made for the organisation should be relevant and adequate to the size and	• Obtain and review the existing disaster recovery/ business resumption plan.

Risk	Control	Audit Guidelines/Procedure
lead to the formulation of a weak and ineffective Plan.	nature of the organisation. Sufficient Risk Assessment and Business Impact Analysis should be performed and documented while revising/ formulating a BCP/DRP.	• Obtain and review plans for disaster recovery/ business resumption testing and/or documentation of actual tests • Obtain and review the existing business impact analysis. • Gather background information to provide criteria and guidance in the preparation and evaluation of disaster recovery/ business resumption plans. • Gain an understanding of the methodology used to develop the existing business impact analysis. • Determine if recommen-dations made by the external firm who produced the business impact analysis have been implemented or otherwise addressed.
Irregular revision of the BCP/DRP would lead to an outdated plan being executed and would be ineffective thus leading to losses and closure of the organisation.	Timely revision of the BCP/ DRP should be carried out. Correct versioning of the plans should be present and the plans of the older versions should be archived and kept away from the latest version.	• Determine if the plan is dated each time that it is revised so that the most current version will be used if needed. • Determine if the plan has been updated within past 12 months.
Employees and other personnel who are ignorant of the plans would lead to lack of co-ordination, chaos and confusion during execution of the BCP/DRP.	Employees should be given periodic briefing about the BCP/DRP. Roles and Responsibilities of each employee should be allotted for smooth execution of BCP.	• Interview functional area managers or key employees to determine their understanding of The disaster recovery/ business resumption plan. Do they have a clear understanding of their role in

Risk	Control	Audit Guidelines/Procedure
	Relevant documents should be made available and kept at strategic areas of the organisation.	working towards the resumption of normal operations? • Determine all the locations where the disaster recovery/ business resumption plan is stored. Are there a variety of locations to ensure that the plan will survive disasters and will be available to those that need them?
Loss of life to the employee is a very serious matter and loss if any is a seriously bad for the image of the company	Employees should be given a first preference while planning the DRP/BCP. Loss of material can be tolerable but loss of life should be avoided.	• Have key employees seen the plan and are all employees aware that there is such plan? ii) Have employees been told their specific roles and responsibilities if the disaster recovery/ business resumption plan is put into effect? • Does the disaster recovery/ business resumption plan include contact information of key employees, especially after working hours? • Does the disaster recovery/ business resumption plan include provisions for people with special needs? • Does the disaster recovery/ business resumption plan have a provision for replacement staff when necessary?
Buildings, electricity, telecommunications, storage facilities, water and other infrastructure if not well provisioned will be a hindrance during the recovery stages.	As feasible by the organisation, adequate measures like having an alternative site fully equipped should be made available. Rent Agreements/leases	• Does the disaster recovery/ business resumption plan have a provision for having a building engineer inspect the building and facilities soon after a disaster?

Risk	Control	Audit Guidelines/Procedure
	to the alternative facility should be maintained. Adequate transport and telecommunication facilities should be available.	so that damage can be identified and repaired to make the premises safe for the return of employees as soon as possible • Does the disaster recovery/ business resumption plan consider the need for alternative shelter, if needed? Alternatives in the immediate area may be affected by the same disaster. • Review any agreements for use of backup facilities. • Verify that the backup facilities are adequate based on projected needs (telecommunications, utilities, etc.). Will the site be secure? • Does the disaster recovery/ business resumption plan consider the failure of electrical power, natural gas, toxic chemical containers, and pipes? • Are building safety features regularly inspected and tested? • Does the plan consider the disruption of transportation systems? This could affect the ability of employees to report to work or return home. It could also affect the ability of vendors to provide the goods needed in the recovery effort.
Inadequate IT Environment at the alternative site could lead to late resumption of the Business.	Care should be taken that alternative IT Infrastructure should be made available at	• Determine if the plan reflects the current IT environment.

Risk	Control	Audit Guidelines/Procedure
	the Alternative site. Provision for Maintenance of the alternative IT Infrastructure should be present.	• Determine if the plan includes prioritisation of critical applications and systems. • Determine if the plan includes time requirements for recovery/availability of each critical system, and that they are reasonable. • Does the disaster recovery/ business resumption plan include arrangements for emergency tele-communications? • Is there a plan for alternate means of data transmission if the computer network is interrupted? Has the security of alternate methods been considered?
Inadequate details about the administration during the time of crisis will lead to execution hindrances. Inadequate Incident Response teams could lead to a higher chaos and lack of co-ordination.	BCP Policy should contain details regarding administration during Crisis, Incident Management, essential records to be preserved for future use. BCP Policy should provide for the protection of critical assets, documents. BCP Policy should provide for the correct storage for such documents.	• Does the disaster recovery/ business resumption plan cover administrative and management aspects in addition to operations? Is there a management plan to maintain operations if the building is severely damaged or if access to the building is denied or limited for an extended period of time? • Is there a designated emergency operations center where incident management teams can coordinate response and recovery? • Have essential records been identified? Do we have a duplicate set of essential records stored in a secure location?

Risk	Control	Audit Guidelines/Procedure
		• To facilitate retrieval, are essential records separated from those that will not be needed immediately? • Has executive management assigned the necessary resources for plan development, concurred with the selection of essential activities and priority for recovery, agreed to back-up arrangements and the costs involved, and are prepared to authorize activation of the plan should the need arise.
Lack of preservation of key business contacts and creation of special reserves could result in an ineffective BCP/DRP Execution.	Ensure that the BCP Policy provides for preservation of contacts either through backups and the management policy has provides for creation of special reserves for BCP/DRP crisis.	• Does the disaster recovery/ business resumption plan include the names and numbers of Suppliers of essential equipment and other material? • Does the disaster recovery/ business resumption plan include provisions for the approval to expend funds that were not budgeted for the period? Recovery may be costly.

Appendix 3: Sample of BCP Audit Finding

Max Infotech should have an alternate disaster recovery site and documented procedures and policies for disaster recovery.

Observation

Max Infotech does not have an alternate disaster recovery site. Also documented Disaster Recovery Plan (DRP) and business continuity plan are not there.

Exposure

The DRP is a key plan ensuring availability of resources critical to the business operations. In the absence of documented procedures and policies for the same, it may be difficult to recover from a disaster resulting in non-availability of data and applications to the users for unacceptable period of time thereby interrupting business processes and impacting the business.

Cause

This is due to lack of documented Disaster Recovery Plan (DRP).

Recommendation

Ensure that the Max Infotech has an alternate disaster recovery site and a documented procedures and policies for disaster recovery. This document should include:

- Provision for back-up and restoration of resources identified as critical to recovery;
- Provision for back-up and off-site location of non-critical application software, data files and system software to facilitate their restoration following the recovery of critical application;
- Frequency of back-up and off-site rotation and number of generations maintained, of production data files including databases;
- Back-up and off-site copies of system software, updated or replaced with each upgrade or revision;
- Off-site copies of systems, programme, user and operations documentation updated to reflect system revision;
- Instructions on how to restore from back-up copies of program and data files.

ISBN: 978-81-8441-335-9

₹ 750/- (For Modules I to VII) with DVD

http://cit.icai.org

www.icai.org

July/2015/P3000(Revised)