

Edition 1
Year of Publication: 2017

© Confidentiality & Proprietary Information

This is a confidential document prepared by iNurture. This document, or any portion thereof, should not be made available to any persons other than the authorised and designated staff of the company/institution/vendor to which it has been submitted.

No part of this document may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of iNurture.

Author's Profile


Mr. Devashish Goswami,


Devashish Goswami adorned his qualification with a Master's Degree in Computer Application (MCA) and M.Phil in Computer Science. He worked as a Computer Faculty in many organisations under Bangalore University as well as a Corporate Trainer. He has overall 8 years of work experience with a blend of corporate and academic.


Being a member of CSI-India, IISC-Bangalore, and IIT-Bombay, he is also a Tech member of ICST-Belgium and IACSIT-Singapore. He has published many papers in various national and international journals in the field of e-Learning, Mobile Computing, Cloud Computing, Network security and ICT. Moreover, he has presented many papers in national and international conferences. His areas of interest are Mobile Computing, Cloud Computing and Network Security. Presently, he is an eLearning – SME at iNurture Education Services Pvt Ltd.


How to use the Self Learning Material


The pedagogy used to design this course is to enable you to assimilate the concepts and processes with ease. The course is divided into **Modules**. Each module is categorically divided into **Chapters**. Each chapter consists of the following elements:


 **Table of Contents:** Every chapter consists of a well-defined table of content. *For example: “1.1.8.(i)” should be read as “Module 1. Chapter 1. Topic 8. (Sub-topic i)” and 1.2.8. (ii) should be read as “Module 1.Chapter 2. Topic 8. (Sub-topic ii)”*


 **Aim:** ‘Aim’ refers to the overall goal to be achieved by going through the chapter.


 **Instructional Objectives:** ‘Instructional Objectives’ defines what the chapter intends to deliver.


 **Learning Outcomes:** ‘Learning Outcomes’ refers to what you will be able to accomplish by going through the chapter.


 **Advantages:** ‘Advantages’ describes the positive aspects of that particular method, theory or practice.


 **Disadvantages:** ‘Disadvantages’ describes the drawbacks of the particular method, theory or practice.


 **Summary:** ‘Summary’ contains the main points of the entire chapter.


 **Self-assessment:** ‘Self-assessment’ contains a set of questions to answer at the end of each topic.

 **e-References:** ‘e-References’ is a list of online resources that have been used while designing the chapter.

 **External Resources:** ‘External Resources’ is a list of scholarly books for additional source of knowledge.

 **Video Links:** ‘Video Links’ contain links to online videos that will help you to understand the concepts better.

 **Did you know? :** ‘Did you know’ is an interesting fact that helps improve your knowledge about the topic.

 **Activity:** ‘Activity’ is used to demonstrate the application of a concept. Activities can be online and offline.

Disaster Recovery and Business Continuity Management

Course Description

Business Continuity and Disaster Recovery (BCDR or BC/DR) are closely related to practices that outline a company's preparation for unexpected risks to sustain operations. Disaster recovery refers to specific steps that have to be taken to continue operations even after a disaster. Business continuity describes the principles and procedures an organisation must put in place to make sure that mission-critical functions can continue throughout and after an event of a disaster. Also, it addresses more comprehensive planning and preparation that focuses on long-term challenges to organisational success. BC/DR must be a key part of a company's overall planning process. Disaster events are unpredictable; hence, it is essential to take an active methodology in the overall planning before it is too late. Failure in any part of the business process can turn into a loss of revenue. However, with a clear and well-thought-out business continuity and disaster recovery plan, a business can moderate the risks and reduce recovery time.

This course describes why BC/DR is essential for an organisation. This course gives a simple outline of business continuity planning. It starts with a brief description of the types of events that can affect the continued operation of a business, then shifts to IT considerations. It also provides solid advice for protecting organisation's critical technology assets and explains how managed solutions can help streamline disaster recovery processes and reduce the burden on internal IT resources. This course describes how to prepare a BC/DR plan for an organisation, conduct training and awareness program for staff members and individuals to protect the assets of an organisation in the event of a disaster.

This course is designed to serve as a stepping stone to the students to build a career in the field of Computer Science and Information Technology.

The **Disaster Recovery and Business Continuity Management** course contains **Five Modules**.

MODULE 1: BUSINESS CONTINUITY MANAGEMENT (BCP)

Introduction to Business Continuity Planning (BCP), Business Resumption Plan (BRP) or Disaster Recovery Plan (DRP), Common terminologies used in BCP and DRP, NIST SP800-34 Emergency Action Plan which includes the phases of Recover/Resume, Protect and Sustain, Causes of Disasters.

MODULE 2: STAGES IN BUSINESS CONTINUITY MANAGEMENT

BCP objectives. Information Protection Environment. Security Technology and Tools. Steps involved in creating a BCP, Phase 1: Project Management and Initiation. Phase 2: Business Impact Analysis. Phase 3: Recovery Strategies, Phase 4: Plan Development and Implementation.

MODULE 3: BUSINESS RECOVERY STRATEGIES

Facility and Supply Recovery strategies. User Recovery strategies. Technical Recovery strategies, Data Recovery strategies, Activation Phase- Major Disaster or Disruption, Intermediate Disaster or Disruption, Minor Disaster, Activating BC/DR Teams, Developing Triggers, Transition Trigger. Defining BC/DR Team and Key Personnel, Defining Tasks, Assigning Resources, Communication Plan.

MODULE 4: TESTING, MAINTENANCE, AWARENESS AND TRAINING MECHANISMS

Different types of tests including structured walk-through, checklist test, simulation, parallel test and full interruption test. Steps required to maintain a BCP.

MODULE 5: PREPARATION OF BCP

Requirements for BCP awareness and training, Conduct a case study of IT Organisation and prepare a Business Continuity Plan for the same using the learning from this course.

Table of Contents

MODULE 1

Business Continuity Management (BCP)

Chapter 1.1 Fundamental of Business Continuity and Disaster Recovery Plan	1
Chapter 1.2 Disasters Causes and Recovery	27

MODULE 2

Stages in Business Continuity Planning

Chapter 2.1 Elements of Business Continuity Planning	49
Chapter 2.2 Business Continuity Planning Strategies	73

MODULE 3

Business Recovery Strategies

Chapter 3.1 Recovery Management and Strategies	95
Chapter 3.2 Phases of Business Continuity Management	115

MODULE 4

Testing, Maintenance, Awareness & Training Mechanisms

Chapter 4.1 Testing and Maintenance of Business Continuity Plan	135
Chapter 4.2 Awareness & Training Mechanisms of Business Continuity Plan	157

MODULE 5

Preparation of Business Continuity Plan

Chapter 5.1 Design of Business Continuity Plan and Training Methodologies	175
Chapter 5.2 Case Study	195

Disaster Recovery and Business Continuity Management

MODULE - I

Business Continuity Management (BCP)

Business Continuity Management (BCP)

Module Description

Business continuity and disaster recovery planning are both essential parts of an organization to reduce the business risk. Since it is not possible to eliminate all the risk factors, companies are implementing both disaster recovery and business continuity plans to fight with the disruptive events. Both the processes are equally important for an organization as they help the organization to recover and resume the business operations after the event of a disaster.

The main goal of studying this module is to understand the concept and need of disaster recovery plan and business continuity plan. Disaster recovery plan specifies how a company should prepare and respond to a disaster and describes the steps that a company may need to take to ensure the recovery of business operations. Disaster recovery planning reduces the long-term negative impact on the business. Business continuity planning proposes a more complete and broad approach to ensure the availability of business operations after the event of a disaster. A business continuity plan considers all the aspects of a business functioning, rather than just technology systems. It specifies the necessary steps a company needs to be take to reduce the effects of a service interruption. It reduces the short-term negative impact on the business.

By the end of this module, students will be able to analyze the role of business continuity plans by validating the steps used in recovery strategies to minimize the effects of a disaster. Also, they will be able to recognize the purpose, scope, and relationship among various plans used in business contingency planning. They will be able to compare various strategies used to ensure the survival of an organization and also, they will be able to identify the various causes of disaster that harm the organizational assets.

Chapter 1.1

Fundamental of Business Continuity and Disaster Recovery Plan

Chapter 1.2

Disasters causes and recovery

Chapter Table of Contents

Chapter 1.1

Fundamental of Business Continuity and Disaster Recovery Plan

Aim.....	1
Instructional Objectives.....	1
Learning Outcomes.....	1
1.1.1 Introduction to Business Continuity Planning (BCP)	5
Self-assessment Questions.....	13
1.1.2 Business Resumption Plan (BRP) or Disaster Recovery Plan (DRP).....	13
Self-assessment Questions.....	18
1.1.3 Common Terminologies used in BCP and DRP.....	18
Self-assessment Questions.....	20
Summary	21
Terminal Questions.....	22
Answer Keys.....	23
Activity.....	23
Bibliography.....	24
e-References.....	24
External Resources	24
Video Links.....	25



Aim

To equip the students with the basic concept of business continuity plan and disaster recovery plan, to develop and test a specific set of plans to protect business operations and also to provide the ways for the recovery of data in case of any accidental damage, loss or failure of facilities



Instructional Objectives

After completing this chapter, you should be able to:

- Explain business continuity plan and its elements
- Identify the scopes and objectives of disaster recovery planning
- Describe the various technical terms used in BCP and DRP creation based on their services and functionalities



Learning Outcomes

At the end of this chapter, you are expected to:

- Analyze the role of a business continuity plan to ensure business processes continue during a time of disaster
- Validate the step by step plan used in recovery strategies to minimize the effects of a disaster
- Identify the scope and objectives of an effective disaster recovery plan which reflects the current state of the business
- Outline the important terminologies that are used in BCP and DRP which will help the business owner take advantage of the business continuity plan

Introduction



It's no secret that every organization believes in the importance of disaster recovery planning. But what does that planning actually look like when it's put to the test in a real-world scenario? We have included some business continuity examples to show how it is helpful for organizations to continue their business critical operations at the time of disaster. Also, it can spoil the reputation of an organization if a business continuity plan is not proper or does not exist.

Example 1: Fire torches office of managed services provider (MSP)

On the night of September 16, 2013, lightning struck an office building in Mount Pleasant, South Carolina, causing a fire to break out. The offices were home to Cantey Technology, an IT company which manages servers and provides services for more than 200 clients.

The fire burned Cantey's network devices, connection cables and computer hardware. The equipment was damaged beyond repair and the office was unworkable. But Cantey's clients did not face any difficulty and never knew the difference. As part of **Cantey's business continuity plan**, they shifted its client servers to a remote data center, where continual backups were taken. Though the staff had to move to a temporary office, their clients never experienced any disturbance in the service.

Example 2: Computer virus infects UK hospital network

This is the worst example of business continuity. In November 2016, a fatal computer virus infected a network of hospitals in the UK, named as “The Northern Lincolnshire and Google NHS Foundation Trust”. The virus damaged hospital systems and stopped all its operations at three different sites for five days. They had to shift all their patients, including those who are in critical condition, to some other hospitals. In a report published by Computing.co.uk it was mentioned that this institution had been no business continuity plan in place. Especially in the context of health care, disaster scenarios can be truly life-or-death situations. Every hospital should have an effective business continuity plan which outlines the necessary measures for responding to a critical IT systems failure. If there had been such a plan in this case, the hospitals could have taken care of their patients better.

Business continuity (BC) and disaster recovery (DR) planning are frequently neglected by organizations. Every year, many members of different organizations report that they are not confident or able to recover and resume business operations after the event of a disaster because of lack of support provided by management. Management does not want to spend much on BC/DR, as BC/DR planning is expensive and there is no immediate return on investment. It is similar to buying insurance -- spending in something we wish we will never need. But, it should not be in that way.

Business owners need to integrate business continuity and disaster recovery plans in their day-to-day business operations. Because of the rapid growth of technology, DR planning has become more affordable and easier nowadays. Business owners are finding different ways to combine disaster recovery with other crucial business operations to integrate business processes. Perfect planning and management are the essential elements for the success of business continuity and disaster recovery. It is not a one-time event and it demands ongoing management.

Thankfully, backups are expanding and getting easier nowadays. Cloud backup and recovery is making it easier than ever before to protect valuable information. There are various backup providers who provide different types of recovery services to the organizations.



10 Most promising disaster recovery solution providers are listed in the figure 1.1.1

Company Name	Description
Arcserve	Provider of next generation data protection solution for virtual and physical environments.
Axcient	Axcient's backup and disaster recovery solution protects data, applications and IT infrastructure from downtime.
Bluelock	Provides cloud based disaster recovery solutions, data centers and security modules for sensitive data that adds to business continuity plan.
Cable & Wireless Communications	Offering disaster recovery as a service (DRaaS) to ensure data back up and security.
Cogeco Data Services and Peer 1	Provider of the solutions, infrastructure and operational expertise to provide turnkey application DR solutions
Continuity CO	A risk management, business continuity and disaster recovery services company that specialize in helping businesses mitigate risk through effective planning and management
Continuum	Continuum is the technology industry's only channel-exclusive provider of fully integrated managed services solutions
Datto	Provides complete system backup and wide-ranging data recovery and business continuity solutions with a Total Data Protection Platform, including a set of software and hardware devices
Evolve IP	One of the nation's fastest growing cloud companies, Evolve IP provides organizations with a unified option for cloud services with its Evolve IP OneCloud™ solution. Today, more than 80,000 users across the globe depend daily on Evolve IP for virtual data...
iland	Provider of DRaaS that creates simple backup files or documents to Enterprise Cloud Services portal in zero Recovery Time and Recovery Point Object

Figure 1.1.1: Some of the promising disaster recovery solution providers

In this chapter, we have discussed the concept of business continuity planning (BCP), elements of BCP and various phases involved in BCP. Also, this chapter covers the concept of disaster recovery plan (DRP), various recovery strategies, steps to create recovery strategies and different terminologies used in BCP and DRP.

1.1.1 Introduction to Business Continuity Planning (BCP)

What is Business Continuity Plan?

The business continuity planning (BCP) is the preparation of methods and procedures to identify threats and risks facing a company and providing solutions to protect company's assets and business operations. Business continuity handles the critical processes that need an

organized structuring to be used at any point of emergency so that business activities can resume. BCP involves understanding the risks and threats that the company may face. It also helps the company come up with a strategy through which the assets and personnel associated with it can be protected so that the business can continue even at the time of a disaster. The companies that invest on establishing good BCP develop better chances of withstanding any form of unpredictable events that disrupt operations. BCP is important for any business and it needs time, effort and money to be invested. The processes in BCP start with finding out the risks, then understanding the impact these risks can create on the business operations, implementing procedures and methods for reducing the risks, testing them to check their effectiveness and then conducting periodic reviews of the whole process for ensuring that they are up-to-date.

a) Element of business continuity planning

To design a potential Business Continuity Plan (BCP), we need to focus on various key elements which help us to drive our business (Figure 1.1.2).

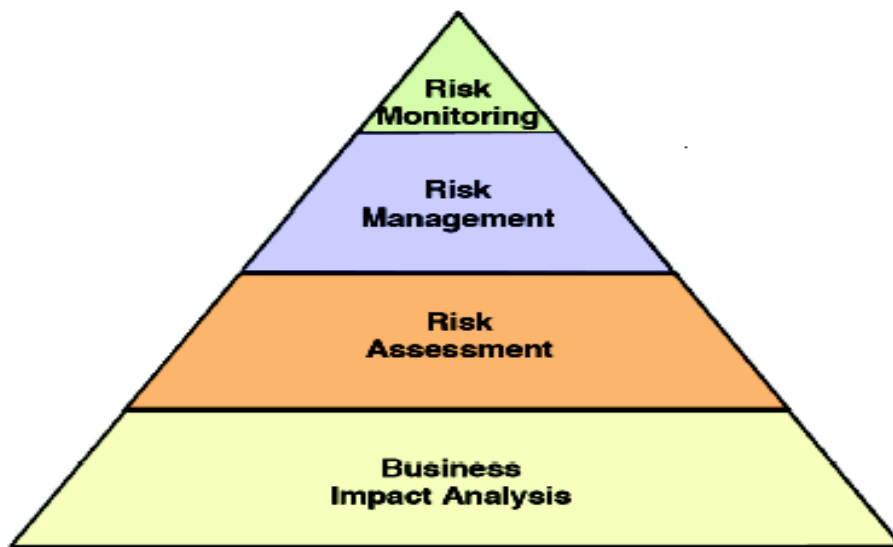


Figure 1.1.2: Element of Business Continuity planning

Business Impact Analysis (BIA)

Business Impact Analysis (BIA) is the first step in developing an effective BCP. We need to conduct a Business Impact Analysis based on the long-term goals of the company. With the help of BIA, a business owner can identify non-specific events of the business processes.

Also, a business owner needs to calculate the organizational risk based on the categories listed below. At the time of evaluating each category, the owner needs to study the possible risk and estimate the maximum amount of time allowable to recover. Further, he has to consider the cost of operational recovery.

The following are the essential components needed for performing this analysis:

- Facilities
- People
- Communication (IT)
- Supply Chain
- Equipment
- Vital Records/Documentation
- Intellectual Property

1. Facilities: It identifies the failure points within the facility and infrastructure design and prepares a recovery plan for these failures.

2. People: Most business operations require well-experienced workforce. Business operations will be impacted if the workforce is not available to support the business operations.

3. Communication: To support clinical and commercial programs, most companies use contract manufacturing (CMO) and research (CRO) organizations. It adversely impacts the organizations if these communications become worse, or if they start losing business data.

4. Supply Chain: Company revenue depends on the supply chain. Procurement, warehousing and material handling are the main parts of a supply chain. In case of a disruption, it affects the supply chain and it might be critical for an organization to find qualified alternate suppliers to continue the business operations.

5. Equipment: Many business processes demand customized equipment to perform the operations. At the time of a disaster, if these processes are transferred to some alternate equipment, it won't behave in the same way and might produce incorrect output.

6. Vital Records/Documentation: One of the most important elements of the business process is its document. All internal and external processes are operated based on these documents. At

the time of a disaster, if an organization fails to recover its critical documents, it might affect both current and future products of the company.

7. Intellectual Property: Because of some Socio-economic issues, if an organization is not able to support customers who depend on them, then they might take the help of multiple manufacturers to support the customers. In such cases, how can company ensure that its rights are protected?

8. Risk Assessment (RA): The Risk Assessment (RA) Phase identifies the business disruption pattern which is common to a business and helps the owner to develop an effective business plan. The owner should not develop the threat scenarios too narrow; otherwise the BCP will not be able to protect the organization completely from a disaster. The RA is responsible for analyzing all the risk related to business, customers, employees and shareholders.

9. Risk Management: After identifying all the threats of an organization, the next step is Risk Management which helps in preparing a business continuity plan. This plan explains all the essential steps to reduce risk. An effective BCP includes strategies, procedures, policies and operations required to recover critical business operations after a disaster. It is not possible to prepare a BCP for every threat, so a BCP should be prepared in such a way that it covers most of the threats possible.

10. Risk Monitoring: The final step is developing a program which ensures that the current plan is efficient enough to perform business operations and remains relevant as the business grows. A business owner needs to review this plan annually to ensure that the policies and procedures involved in this plan reflect the current needs of the company. The BCP Process flowchart is shown in the figure 1.1.3 which contains all the four elements of BCP.



Figure 1.1.3: All four elements of BCP

Example: Risk Management**Bank of America**

In 2012, BofA decided to charge \$5 per month for each of the customer to gain access to their funds via their debit cards.

BofA might have thought that initially some of the customers will raise the issue and later everything will be fine as people don't have time to change the bank or come to the bank to speak about this issue. However, it was a horrible mistake on the part of BofA, the reaction from customers was far greater than they ever imagined.

BofA couldn't deny two major dates i.e. November 5, 2011 "Bank Transfer Day" and November 8, 2011 "Dump Your Bank Day" and both had been started by ordinary citizens protesting the debit card charge.

It was a poor idea on the part of BofA to charge \$5 per month for each of the customer to gain access to their funds via their debit cards, in a time when every American was looking keenly at each and every dollar being spent.

BofA would not have thought about the average customer of the bank and their reaction on this issue. They would have seen the negativity and dumped the idea if they had a risk management plan in place. It would have saved BofA from losing a lot of customers.

All project leaders, teams and stakeholders need to consider risk management during project initiation. When risk management is not considered properly, things don't go well.

b) Phases of BCP

The process of BCP can be categorized into different phases which include recovery, continuation and also the preservation of the whole business operation. It is not just limited to the technical component. There should appropriate plans involved in it which can be of help in protecting all the resources of an organization -- IT infrastructure, finance, human resource

-- at any disastrous incident. Business continuity planning can be divided into seven stages as shown in the figure 1.1.4

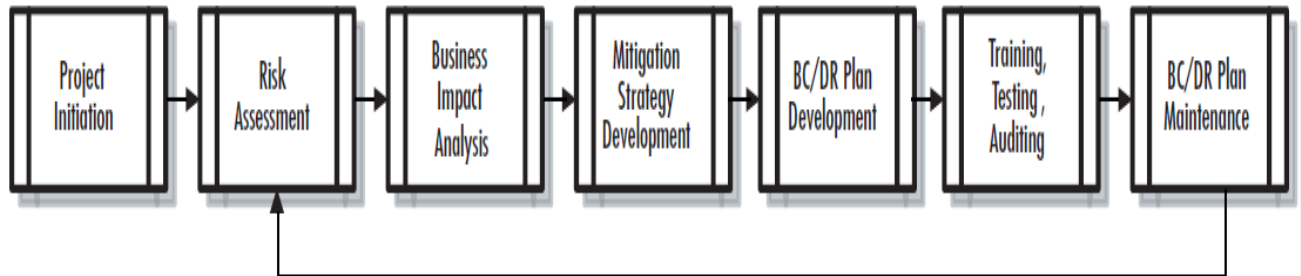


Figure 1.1.4: Seven stages of BCP

- **Project Initiation**

Project initiation is indeed an important phase in Business Continuity or Data Recovery planning. If the process included in the BCP needs to be created or implemented, it is necessary to have cooperation from the whole organization. Different projects may need different applications and the knowledge of how they work or how they need to be backed up are things that will only be known to the experts in that niche. The project initiation ensures collaborating with different departments and executives for contributing toward the Disaster Recovery or Business Continuity.

- **Risk Assessment**

Risk assessment is the phase in which key members who work for business continuity process have brainstorming sessions to analyze the potential risks that company may face. IT experts and experts from marketing, transportation and all other areas included in an organization need to be a part of such discussions. The risks which may be getting analyzed can be anything from fire to catastrophic disasters like earthquake. The expert advice from varying niches can help in collaboratively assessing the impact of these unpleasant events.

- **Business Impact Analysis**

Once the business owner understands the risks that may hit the organization, there should be an analysis done on how far it is going to hit the business. There should be an assessment done on how the business is going to get impacted by such an incident.

For example, there may be certain servers or applications which, when affected badly, can seriously hamper the company's business. Servers "going down" is disruptive but when this happens to some key servers, the impact cannot be tolerated by the business of the company. The experts in the company can help in understanding these facts and prioritizing the strategies for business continuity.

- **Development of Mitigation Strategy**

If it is a small company, mitigation strategy may be very simple, requiring only the creation of several copies of critical information and saving it in different places. For huge corporations, the process can be very complicated. For each of the risk identified, there may be a significant impact on the business. It is necessary for them to find out the options so that risk, as well as the impact created by it, can be handled, reduced, transferred or even avoided.

- **Plan Development**

Once the analysis is carried out, the next phase is to develop a plan. Similar to any other plan, it is necessary to create an outline of the methodology that is going to be followed so that you get better chances to be successful. This also reduces the occurrences of errors and gaps. Plan development involves standard processes including quality metrics, timeline, budget, defining scope, developing technical and business requirements and so on.

- **Training, Auditing & Testing**

It is good to create scenario-based case studies for the plan developed so that it can be easier for training people on the plan. It is also necessary to use simulations and exercises for those events and disasters that have got a higher probability of occurrence.

- **Plan Maintenance**

There should be someone within the company who actually maintains the plan that is created. If there are no proper directions on maintaining the plan that is created, then all the efforts put towards it may go in vein. In this case, the disaster recovery may be of no help to the company when any disaster actually strikes. It is not a complicated process but maintaining the plan is indeed an important step.



Self-assessment Questions

- 1) Which of the following is not a part of business continuity planning?
 - a) Business Impact Analysis
 - b) Risk Assessment
 - c) Risk Management
 - d) Risk Analysis

- 2) The _____ phase identifies the business disruptions which are common to a business and helps the owner to develop an effective business plan
 - a) Risk Assessment
 - b) Risk Analysis
 - c) Risk Management
 - d) Risk Identification

- 3) Which of the following is not a phase of business continuity planning?
 - a) Plan Development
 - b) Plan Maintenance
 - c) Risk Monitoring
 - d) Risk Assessment

1.1.2 Business Resumption Plan (BRP) or Disaster Recovery Plan (DRP)

Disaster Recovery Plan is a documented and structured approach which involves instructions which can be useful in the events of any disaster. The plan may include step by step instructions which can help in reducing the effects of the disaster so that the organization may be able to continue operating or may be able to, at least, resume the critical functions as soon as possible. Disaster recovery planning includes analysis in terms of the business processes as well as continuity needs. An organization should do risk analysis and business impact analysis for establishing recovery time objective and recovery point objective which can be of great help in generating the detailed plan for disaster recovery.

Recovery Strategies

A disaster recovery strategy needs to be started at the business level through a determination of the applications that are very important for running organization. Recovery time objective (RTO) helps in describing the target amount time the business application can actually be down. It can be measured in terms of seconds, minutes and hours. Recovery point object (RPO) defines the previous point to which the application should be restored or recovered. Recovery strategies should define the plans of the organization in responding to the incident when disaster recovery plans can describe the way organization should be responding. The

organization needs to consider the factors like suppliers, data and technology, management's position on risks, resources and budget before they determine the recovery strategy. It is important that the recovery strategies get approval from the management. The strategies should match the goals of the organization. The disaster recovery strategies which get developed and approved can be converted to disaster recovery plans.

Disaster Recovery Planning Steps

The process of disaster recovery plan is not just about creating documentation. Prior to documentation, there are other phases like risk analysis and business impact analysis that help in determining where the resources should be focused in the process of disaster recovery planning. BIA helps in identification of impacts associated with various disruptive events and it is the point at which risks are identified within the disaster recovery process. It even helps in generating RPO and RTO. Risk analysis (RA) finds out the vulnerabilities and threats which can disrupt any operations associated with the systems and the processes which are mentioned in BIA. RA can even analyze the probability of the occurrence of a disruptive event and give an outline on the chance of potential severity.

The checklist for DR plan includes:

- Establishing the activity's scope
- Gathering documents relevant to network infrastructure
- Finding out critical vulnerabilities, threats, and assets
- Reviewing the past outages and incidents that were unplanned and the way they were handled.
- Identifying the DR strategies
- Creating a team for emergency response
- Ensuring that the disaster recovery plan is reviewed and approved by management
- Testing the plan
- Updating the plan
- Implementing audit on the DR plan.

Disaster recovery plans are very important and live documents. Getting employees at all the levels of the organization involved in it can help in giving more value to it.

Creating Disaster Recovery Plan

The disaster recovery plan of an organization should start with a summary explaining the important action steps and the important contacts so that the information can be easily accessed. The disaster recovery team and their responsibilities should be defined in the plan. It should also give an outline of the criteria for implementation of the plan. The plan also should include recovery activities and the way to respond to incidents in a detailed way.

Following are other aspects covered in the plan:

- DR policy statement and statement of the intent
- Tools for authentication like passwords
- The goals of the plan
- Geographical factors and risks
- The history of the plan
- Action steps and also legal and financial information.

Objectives and Scope of DR Planning

The disaster recovery plan can vary in their scope from being basic to comprehensive. Some of the DRPs can be of 100 pages long. The budgets for DR may fluctuate with time. Organizations can make use of the free resources. Free information and articles on how to prepare a disaster recovery plan can be found in abundance over the web by reputed sources like disaster recovery Institute International. The goals of DR plan should include identification of critical IT systems, prioritization of RTP, outlining of steps required for restarting, reconfiguring and the recovery of the networks and systems. The primary aim of the plan should be to minimize the negative effects that the disaster can create for the business operations. Employees should be educated about the basic steps to be taken in case of an unpredictable incident. Distance is one of the primary factors to be considered when choosing a DR site.

Types of Disaster Recovery Plans

DR plans can be customized to serve the needs of different environments.

Different types of disaster recovery plans are discussed below:

- **Virtualized Disaster recovery plan:** Virtualization can make disaster recovery a very easy process. A virtualized environment can easily create instances of new VMs in a

matter of minutes and can even help in application recovery by being highly available. It is very easy to test it but it is necessary that the DR plan have the ability for validating whether it is possible for applications to run in the DR mode. It can also help in going through the normal operations within RTO and RPO.

- **Network disaster recovery plan:** If the complexity of the network increases, then creating a plan for recovering the network can also turn out to be a difficult process. Each and every step in the recovery process should be defined in detail and be properly tested and updated. Data that is available in this plan should be specific to a network which the 'networking and performance' staff can understand and implement.
- **Cloud disaster recovery plan:** This disaster recovery plan includes various things like having a backup file on the cloud to get a complete replication done. Cloud DR is cost, time and space efficient but proper management is necessary for maintaining such a plan. The manager should have the idea about where physical and virtual servers are located. This plan should even include security which needs to be reinforced with proper testing.
- **Data center disaster recovery plan:** This is the plan that should be developed for the infrastructure and facility in the data center. The major element of such a plan is operational risk – assessment. It can analyze major components like office space, security, power systems, protection and building location. The plan should be able to cover varying scenarios.

5 Questions business owner need to ask Before Selecting a Backup and Disaster Recovery Solution

QUESTION 1: How much and what kinds of data do you need to back up, and how quickly?

Business owners need to determine the quantities and kinds of data needed to be backed up. It helps the owner to choose the vendor and plan accordingly. Also, the owner needs to specify what type of data he needs to back up such as programs, files, or entire operating system.

QUESTION 2: How much time and how many people are available to set up and operate any solution?

Business owners should know the availability of the resources. Resource includes physical assets of the organization, workforce and time. They should also figure out the amount of resources available for implementing and operating a new backup and disaster recovery solution.

QUESTION 3: How much and what kinds of support will you need?

Support can be of different types such as technical support, backing up applications, support, backing up operating systems support, internal and external audit assistance, assistance with disaster recovery etc. Requirement of support is different for different operating systems. The business owner should specify what type of support he requires for his disaster recovery plan and what should be the resource requirement for it.

QUESTION 4: What will your business need to back up in the future?

No business can remain static for long. So business owners need to take long term decisions while planning for any kind of solution or strategy. It's better to identify the type of data, programs, and operating systems that require to be backed up within the lifetime of the solution.

QUESTION 5: How much are you willing to pay?

Cost analysis need to be conducted by the owner of the business before opting for any service as funding facility vary from company to company. He might go with a cheaper solution also. However, it should be able to back up and restore critical types of data after a disaster.

Business Continuity Management (BCM)	A <i>management</i> process which identifies the risk, vulnerabilities and threats, and provides a framework for creating organizational resilience and buffers the efficiency for an active response.
Business Continuity Plan (BCP)	A set of procedures which guide organizations to recover and resume the business operations in the event of a disaster.
Business Continuity Strategy	A specific approach developed by the organization to ensure its recovery and continuity in the event of a disaster.
Business Impact Analysis (BIA)	A systematic process to identify and validate the potential effects of an interruption to critical business operations as a result of a disaster.
Business Recovery	Steps that are taken to recover and resume the business operations within an acceptable timeframe at the time of a disaster.
Contingency Planning	The process of making arrangements and procedures which make the organization capable of responding to a disaster.
Disaster	A serious disruption of the functioning of a business involving widespread human, material, economic or environmental loss which adversely impacts the ability of the business to cope using its own resources.
Disaster Recovery (DR)	The policy and procedure to preparing for recovery of business operations after a disaster.
Disaster Recovery Plan (DRP)	A management approved document which defines the resources, task, actions, processes and data required to manage the technology recovery effort
Gap Analysis	A survey whose aim is to identify the differences in business processes between before and after a disaster.
Objective	The goal of an organization
Recovery Point Objective (RPO)	The point in time to which business operations are recovering and resume after a disaster.
Recovery Time Objective (RTO)	The time period within which business operations should be recovered after a disaster.
Risk Analysis	The calculation of the risk of threats to an organization



Summary

- Business continuity handles the critical processes which need an organized structuring to be used at any point of the emergency so that business activities can resume.
- BCP is important for any business and it needs time, effort and money spent on the processes.
- Business Impact Analysis (BIA) is the first step of developing an effective BCP.
- With the help of BIA, business owners can identify non-specific events of the business processes.
- After identifying all the threats of an organization, the next step is Risk Management which helps in preparing a business continuity plan.
- Risk monitoring is the final step used to developing a program which ensures that the current plan is efficient enough to perform business operations and remains relevant as the business grows.
- The process of BCP can be categorized into different phases which include recovery, continuation and preservation of the whole business operation and not just focused on the technical component.
- Project initiation is indeed an important phase in Business Continuity or Data Recovery planning.
- Risk assessment is the phase in which key members who work for the business continuity process have brainstorming sessions to analyze the potential risks that company may face.
- If case of a small company, mitigation strategy may be very simple and may need only the creation of several copies of critical information and saving it in different places.
- It is good to create scenario-based case studies for the plan developed so that it can be easier for training people on the plan.

- Disaster Recovery Plan is the documented and structured approach which involves instructions which can be useful in the event of any disasters.
- A disaster recovery strategy needs to be started at business level by determining the applications that are very important for running organization.
- The process of disaster recovery planning is not about just creating documentation. Prior to documentation, there are other phases like risk analysis and business impact analysis that helps in determining where the resources should be focused in the process of disaster recovery planning.
- Disaster recovery plan of an organization should start with a summary explaining the important action steps and the important contacts so that the important information can be easily accessed.
- The disaster recovery plan can vary in their scope from being basic to comprehensive.
- Testing is an important phase in the DR plan as this assures that the plan is free from any kind of deficiencies because the issues can be fixed at the time of testing.



Terminal Questions

1. What is a business continuity plan and why it is important for an organization?
2. Explain various elements of business continuity planning.
3. Explain different phases of BCP.
4. Explain the need of disaster recovery plan.
5. Explain any 10 terminologies used in BCP.



Answer Keys

Self-assessment Questions	
Question No.	Answer
1	d
2	a
3	c
4	a
5	c
6	a
7	c
8	a
9	a



Activity

Activity Type: Offline

Duration: 45 Minutes

Description: Create a disaster recovery plan for an IT company by considering the below mention factors

- People
- Physical Security
- Technology
- Data Supplier
- Policy and procedure

Bibliography



e-References

- *The Four Phases of a Business Continuity Plan*, Retrieved on 23 May 2017, from <http://www.emergency-response-planning.com/blog/bid/32916/the-four-phases-of-a-business-continuity-plan>
- *Disaster recovery plan*, Retrieved on 23 May 2017, from <http://searchdisasterrecovery.techtarget.com/definition/disaster-recovery-plan>
- *Glossary of business continuity terms*, Retrieved on 24 May 2017, from https://www.drj.com/downloads/drj_glossary.pdf
- *Integrating Business Continuity as Part of Strategic Planning*, Retrieved on 24 May 2017, from <http://www.cemag.us/article/2008/04/integrating-business-continuity-part-strategic-planning>
- *BCP*, Retrieved on 24 May 2017, from http://www.webopedia.com/TERM/B/Business_Continuity_Planning_BCP.html

Image Credits

- Figure 1.1.1: <http://disaster-recovery-services.cioreview.com/vendors/most-promising--disaster-recovery-solution-providers-2015.html>
- Figure 1.1.2 and 1.1.3: <http://www.cemag.us/article/2008/04/integrating-business-continuity-part-strategic-planning>.



External Resources

- Susan Snedaker (2013), *Business Continuity and Disaster Recovery Planning* (2nd edition) Syngress.
- Harvard Business School (2004), *Crisis Management Mastering Skills*, Harvard Business Press
- Jon William Toigo (2012), *Disaster Recovery Planning: Preparing for the unthinkable* (3rd Edition),



Video Links

Topic	Link
Business Continuity Management 1 - Intro, Life Cycle, Planning, Scope	https://www.youtube.com/watch?v=25EhtuE3XkE
Business Continuity Management 2 - Impact Analyses	https://www.youtube.com/watch?v=qY4Z42bmVNY
Business Continuity Management 3 - Business Continuity Planning	https://www.youtube.com/watch?v=gBtNesRrk6s
Business Continuity Management 4 - The Traditional and the TIMBUS Way	https://www.youtube.com/watch?v=2yimlwfEJtU



Notes:

