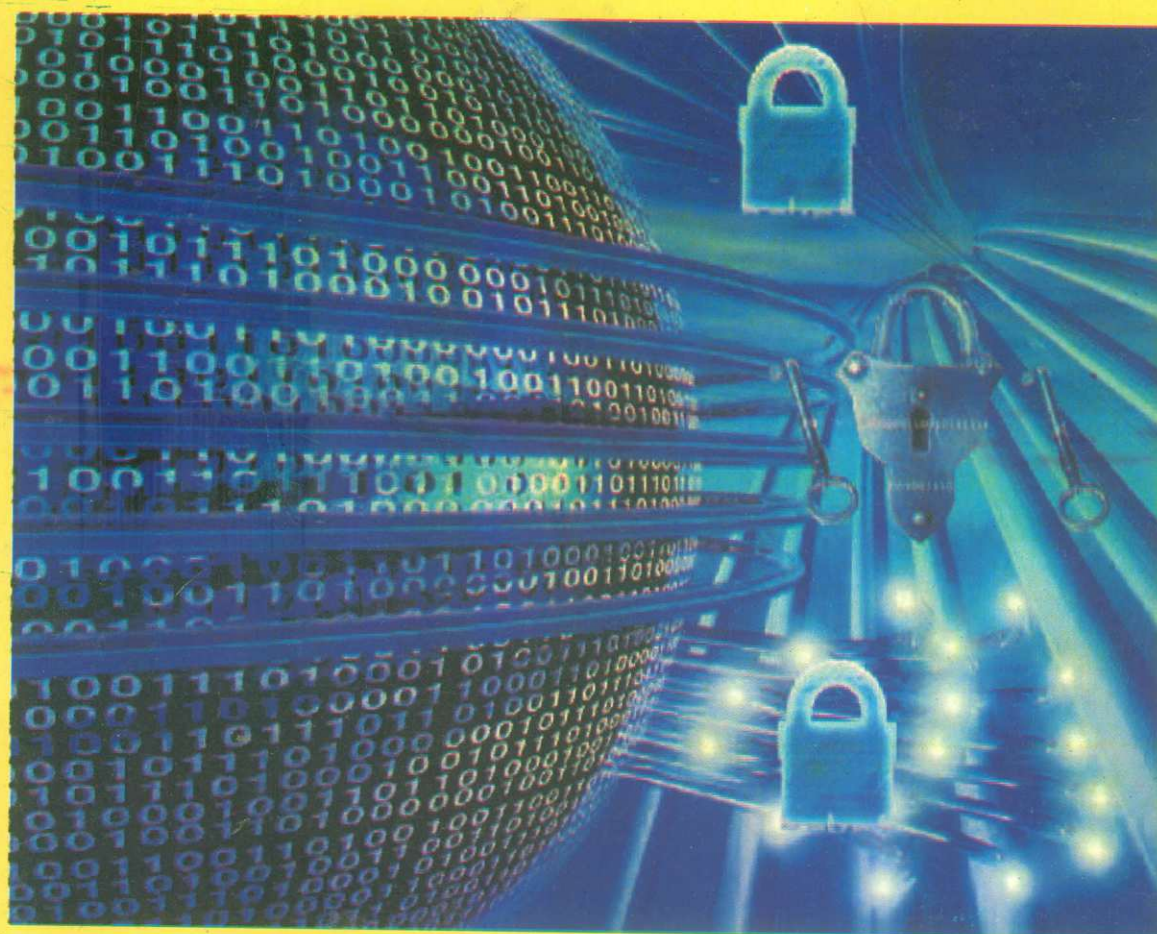




“शिक्षा मानव को बन्धनों से मुक्त करती है और आज के युग में तो यह लोकतंत्र की भावना का आधार भी है। जन्म तथा अन्य कारणों से उत्पन्न जाति एवं वर्गगत विषमताओं को दूर करते हुए मनुष्य को इन सबसे ऊपर उठाती है।”

— इन्दिरा गांधी

“Education is a liberating force, and in our age it is also a democratising force, cutting across the barriers of caste and class, smoothing out inequalities imposed by birth and other circumstances.”

— Indira Gandhi

Block**2****BUSINESS CONTINUITY**

UNIT 1

Need for a Business Continuity Program	5
---	----------

UNIT 2

Overview of Business Continuity Management Life Cycle	30
--	-----------

UNIT 3

Defining Organization's Business Continuity Requirements	66
---	-----------

UNIT 4

Identifying and Selecting Business Continuity Strategies	118
---	------------

Programme Expert/ Design Committee of Post Graduate Diploma in Information Security (PGDIS)

Prof. K.R. Srivathsan
Pro Vice-Chancellor, IGNOU

Mr. B.J. Srinath, Sr. Director & Scientist 'G', CERT-In, Department of Information Technology, Ministry of Communication and Information Technology Govt of India

Mr. A.S.A Krishnan, Director, Department of Information Technology, Cyber-Laws and E-Security Group, Ministry of Communication and Information Technology, Govt of India

Mr. S. Balasubramony, Dy. Superintendent of Police, CBI, Cyber Crime Investigation Cell, Delhi

Mr. B.V.C. Rao, Technical Director, National Informatics Centre, Ministry of Communication and Information Technology

Prof. M.N. Doja, Professor, Department of Computer Engineering, Jamia Milia Islamia, New Delhi

Dr. D.K. Lobiyal, Associate Professor, School of Computer and Systems Sciences, JNU New Delhi

Mr. Omveer Singh, Scientist, CERT-In, Department of Information Technology, Cyber-Laws and E-Security Group, Ministry of Communication and Information Technology, Govt of India

Dr. Vivek Mudgil, Director, Eninov Systems Noida

Mr. V.V. Subrahmanyam, Assistant Professor School of Computer and Information Science IGNOU

Mr. Anup Girdhar, CEO, Sedulity Solutions & Technologies, New Delhi

Prof. A.K. Saini, Professor, University School of Management Studies, Guru Gobind Singh Indraprastha University, Delhi

Mr. C.S. Rao, Technical Director in Cyber Security Division, National Informatics Centre, Ministry of Communication and Information Technology

Prof. C.G. Naidu, Director, School of Vocational Education & Training, IGNOU

Prof. Manohar Lal, Director, School of Computer and Information Science, IGNOU

Prof. K. Subramanian, Director, ACIIL, IGNOU Former Deputy Director General, National Informatics Centre, Ministry of Communication and Information Technology, Govt. of India

Prof. K. Elumalai, Director, School of Law IGNOU

Dr. A. Murali M Rao, Joint Director, Computer Division, IGNOU

Mr. P.V. Suresh, Sr. Assistant Professor, School of Computer and Information Science, IGNOU

Ms. Mansi Sharma, Assistant Professor, School of Law, IGNOU

Ms. Urshla Kant
Assistant Professor, School of Vocational Education & Training, IGNOU
Programme Coordinator

Block Preparation

Unit Writers

Mr. Vijay Singhal
Assistant Professor, Tecnia
Institute of Advanced Studies
Madhuban Chowk, Rohini
Delhi (Unit 1)

Mr. Sumit Chauhan
Assistant Professor (IT)
Management Education &
Research Institute
New Delhi (Unit 2)

Ms. Ritu Aggrawal
Assistant Professor & MCA-
Coordinator, Management
Education & Research Institute
Delhi (Unit 3)

Ms. Rakhee Chhibber
Assistant Professor, Rukmini
Devi Institute of Advanced
Studies, Madhuban Chowk
Rohini, Delhi (Unit 4)

Block Editor

Ms. Urshla Kant
Assistant Professor, School of
Vocational Education &
Training, IGNOU

Proof Reading

Ms. Urshla Kant
Assistant Professor, School of
Vocational Education &
Training, IGNOU

PRODUCTION

Mr. B. Natrajan
Dy. Registrar (Pub.)
MPDD, IGNOU

Mr. Jitender Sethi
Asstt. Registrar (Pub.)
MPDD, IGNOU

Mr. Hemant Parida
Proof Reader
MPDD, IGNOU

November, 2011

© Indira Gandhi National Open University, 2011

ISBN: 978-81-266-5714-8

All rights reserved. No part of this work may be reproduced in any form, by mimeograph or any other means, without permission in writing from the Indira Gandhi National Open University.

Further information on the Indira Gandhi National Open University courses may be obtained from the University's office at Maidan Garhi, New Delhi-110 068 or the website of IGNOU www.ignou.ac.in

Printed and Published on behalf of the Indira Gandhi National Open University, New Delhi, by the Registrar, MPDD.

Printed at : Young Printing Press, 2626, Gali No.7, Bihari Colony, Shahdara, Delhi – 11 00 32

BLOCK INTRODUCTION

This block deals with the Business Continuity. We live in a highly competitive world and so do the business entities. Businesses have to constantly innovate to meet their objectives of providing essential and unique services to their customers. There is no doubting the fact that the technological advances have enabled them to achieve their varied strategies. The threats of disaster, on account of business interruption, are also not extinct – and in fact, they have also evolved along with the technology. Business Continuity Program (BCP) is the standard method by which businesses plan for continuing operations in an emergency. BCP involves several steps, which include performing a Business Impact Analysis (BIA) and a Risk Assessment (RA). It is impossible to properly plan for a disaster if the likely impacts of various disruptions on an organization are unknown. A BIA is a means of systematically assessing the potential impacts of various events on operations. It allows an organization to understand the degree of loss that could occur from each potential disruption. This block comprises of four units and is designed in the following way;

The **Unit One** presents the need of Business Continuity Program from a point of view of both the user as well as the management. The BCP is a standard method by which businesses plan how to continue operations even in the times of emergency / uncertainty. When the Risk Assessment and Business Impact Analysis phases are over, what stand out are the essentials to keep the business moving.

The **Unit two** is an effort towards answering some of the fundamental queries about Business Continuity Management Life Cycle. Here in this unit we have done an attempt to provide knowledge to our learners regarding Business Continuity Planning (BCP) and Business Continuity Planning Process. We have also covered the topics like audit and its types.

The **Unit three** defines organization's Business Continuity requirements. The organization's security policy should be reviewed to determine the confidentiality, integrity, and availability needs of the organization. The appropriate physical, technical, and administrative controls can then be selected to provide the required level of information protection, as stated in the security policy. Business continuity professionals should collaborate with information security professionals to raise awareness of security and to provide training for all employees with the goal to reduce the risks to the organization.

The **Unit four** covers Business Continuity strategies. Many companies associate disaster recovery and business continuity only with IT and communications functions and miss other critical areas that can seriously impact their business. All areas require a clear well thought out strategy based on recovery time objectives cost and profitability impact. Strategy selection involves focusing on key risk areas and selecting a strategy for each one. The primary goals are to maintain business continuity in the face of a disruption or disaster to recover, to key business functions quickly and to mitigate damages.

Hope you benefit from this block.

ACKNOWLEDGEMENT

The material we have used is purely for educational purposes. Every effort has been made to trace the copyright holders of material reproduced in this book. Should any infringement have occurred, the publishers and editors apologize and will be pleased to make the necessary corrections in future editions of this book.

UNIT 1 NEED FOR A BUSINESS CONTINUITY PROGRAM

Structure

- 1.0 Introduction
- 1.1 Objectives
- 1.2 Fundamental Concepts of BCP
- 1.3 Developing Business Continuity Program
- 1.4 Business Continuity Program Stages
 - 1.4.1 Initiation
 - 1.4.2 Risk Assessment
 - 1.4.3 Business Impact Analysis
- 1.5 BCP Goals and Activities
 - 1.5.1 Prevention
 - 1.5.2 Response
 - 1.5.3 Resumption
 - 1.5.4 Recovery
 - 1.5.5 Restoration
- 1.6 Building Disaster Recovery Plan
- 1.7 Assessment of BCP Readiness of an Organization
- 1.8 Let Us Sum Up
- 1.9 Check Your Progress: The Key
- 1.10 Suggested Readings

1.0 INTRODUCTION

"Business Continuity Program is the act of proactively working out a way to prevent, if possible, and manage the consequences of a disaster, limiting it to the extent that a business can afford."

We live in a highly competitive world and so do the business entities. Businesses have to constantly innovate to meet their objectives of providing essential and unique services to their customers. There is no doubting the fact that the technological advances have enabled them to achieve their varied strategies. The threats of disaster, on account of business interruption, are also not extinct – and in fact, they have also evolved along with the technology. Business interruption does happen – but what is of significance is, how much of the consequences of such interruptions can the business afford and whether the business is ready to handle and overcome such eventualities in minimum possible time.

1.1 OBJECTIVES

After studying this unit, you should be able to:

- understand the need of Business Continuity Program;
- explain different activities related to BCP;
- understand the concepts and tools available for BCP;
- outline various BCP goals and activities; and
- perform BCP readiness of an organization.

1.2 FUNDAMENTAL CONCEPTS OF BCP

Business Continuity Program (BCP) is the standard method by which businesses plan for continuing operations in an emergency.

BCP involves several steps, which include performing a Business Impact Analysis (BIA) and a Risk Assessment (RA). It is impossible to properly plan for a disaster if the likely impacts of various disruptions on an organization are unknown.

A BIA is a means of systematically assessing the potential impacts of various events on operations. It allows an organization to understand the degree of loss that could occur from each potential disruption.

The first step in conducting a BIA is identifying the assets that are required to perform the organization's core mission. The second step involves identifying the potential hazards or threats to these assets. The third step requires determining the susceptibility of the organization to the effects of each hazard or threat. The fourth and final step requires determining the potential impact of each threat. Assessing the impact of an event includes not only estimating the quantitative or economic losses but also the qualitative impact on the organization's ability to operate, i.e., psychological effects on employees and effect on the reputation of the organization.

Although the BIA and RA are two separate inquiries, they are closely related and essential steps in BCP; thus, they are often performed together and the terms are used interchangeably. Often, the RA is performed together with the vulnerability assessment in a BIA.

There are various threats and vulnerabilities to which business today is exposed. They could be catastrophic events such as floods, earthquakes, or acts of terrorism, an accidents or sabotage or outages due to an application error, hardware or network failures.

Some of them come unwarned. Most of them never happen. The key is to be prepared and be able to respond to the event when it does happen, so that the organization survives; its losses are minimized; it remains viable and it can be "business as usual", even before the customers feel the effects of the downtime. An effective Business Continuity Program serves to secure businesses against financial disasters. The bonus is customer satisfaction, enhanced corporate image and no dip in the market share.

Standard BCP Model

A general BCP model incorporates the Prevention, Preparedness, Response and Recovery (PPRR) framework. Each of the four key elements is represented by a subtask in the Business Continuity Program.

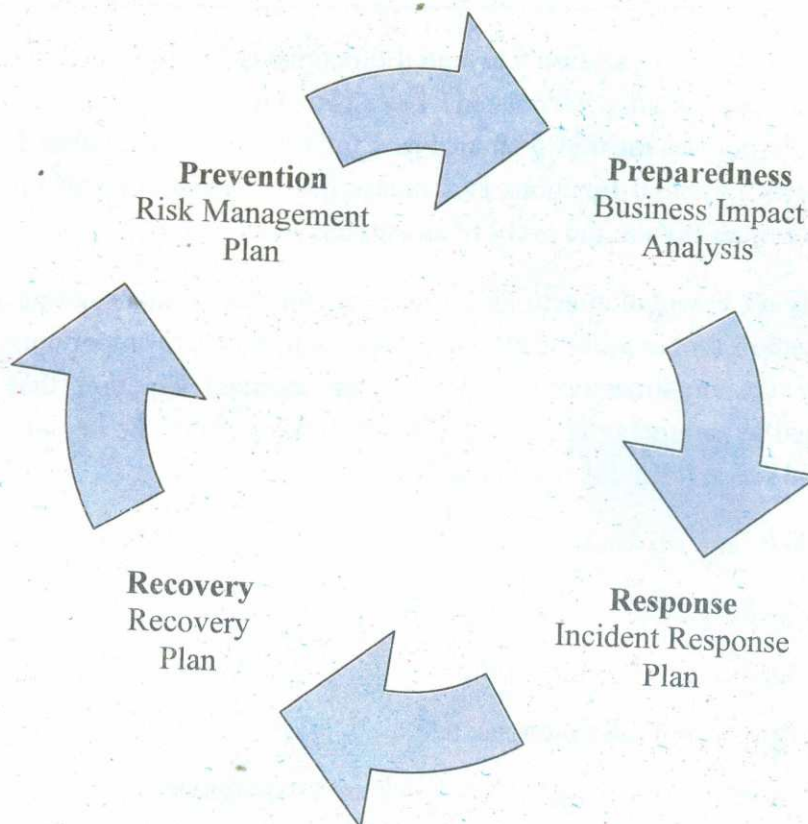


Fig. 1: Business Continuity Program Cycle (PPRR model)

- **Prevention - Risk Management planning**
 - Incorporates the Prevention element that identifies and manages the likelihood and/or effects of risk associated with an incident.
- **Preparedness - Business Impact Analysis**
 - Incorporates the Preparedness element that identifies and prioritises the key activities of a business that may be adversely affected by any disruptions.

- Response – Incident Response planning
 - Incorporates the Response element and outlines immediate actions taken to respond to an incident in terms of containment, control and minimising impacts.
- Recovery - Recovery planning
 - Incorporates the Recovery element that outlines actions taken to recover from an incident in order to minimise disruption and recovery times.

1.3 DEVELOPING BUSINESS CONTINUITY PROGRAM

Identifying the organization's essential functions is a critical step in developing a Continuity Plan. Associated key personnel and supporting critical systems/processes must also be analysed for sufficient period after a disruption is noticed. Essential functions encompass those critical areas of business that must continue even in the event of an emergency.

Identifying essential functions requires an intimate understanding of all the organization's operations. Although many functions are important, not every activity the organization performs is an essential function that must be sustained in an emergency for more than ten days. Thus, the key to identifying essential functions is the organization's mission.

This can be summarised into a four-step approach.

- 1) Identify all functions;
- 2) Identify essential functions;
- 3) Prioritize those functions; and
- 4) Determine essential function resource requirements.

We will also study the documentation format to support each specific step in BCP.

Step 1: Identify All Organization Functions

The mission statement clearly outlines the basic purpose of the organization and is the first place to look to determine essential functions. Existing SOPs, EOPs and reports on operations usually offer a good starting point for identifying various functions.

Once all the functions are identified for Business Continuity Program purposes, narrow the list to only the essential functions. This can be accomplished by

referring back to the organization's mission and considering the beneficiaries of the function. For example, if other organizations or individuals are dependent on a particular function to continue their operations, then the function is probably an essential function.

Table 1: Format for Identifying Organization functions

All Functions (Column 1)	Description of Function (Column 2)	Essential Function?
Database Entry	Entries are made by clerks	Yes

Step 2: Identify Critical Processes and Services

After the essential functions are determined, examine the processes and services that support them. Essential functions and their supporting processes and services are intricately connected. Each essential function has unique characteristics and resource requirements, without which the function could not be sustained. Those processes and services described for each function that are necessary to assure continuance of an essential function are considered critical. Often, critical processes and services vary depending upon the emergency or if they have a time or calendar component.

Essential Function: Backup of Database

Table 2: Format for Identifying critical processes and services

Description of Function (Critical Process or Service)	RTO	Priority	Equipment and Systems
Daily Backup	2 Hours	Medium	Servers and Network
Weekly backup	1 Day	High	Servers and Network

Step 3: Identify Priority of Essential Functions

Once all essential functions and their supporting critical processes and services have been identified, prioritize the functions according to those activities that are pivotal to resuming operations when a catastrophic event occurs.

Prioritization requires determination of time criticality of each essential function and sequence for recovery of essential functions and their critical processes.

An essential function's time criticality is related to the amount of time that function can be suspended before it adversely affects the organization's core mission.

Time criticality can be measured by either recovery time or recovery point objectives. These are terms of art borrowed from Information Technology (IT) disaster recovery planning, but can be used in the broader context of Business Continuity planning.

Recovery Time Objective

A recovery time objective (RTO) is the period of time within which systems, processes, services, or functions must be recovered after an outage.

Recovery Point Objective

A recovery point objective (RPO) is more specific to information systems. It is the amount of data that can be lost measured by a time index. Thus, an RPO of one hour means that the last hour of data before the failure will not be recovered.

Not all processes have RPOs, and some processes can have both a RPO and a RTO. During Business Continuity planning, organizations will primarily be focusing on RTO, but it is important to understand RPO and incorporate RPO information into the COOP where necessary.

Table 3: Format for Identifying Priority of Essential functions

Essential Function	Priority

Step 4: Identify Critical Data Needs

The next step is identification of critical data needs that can take care of the protection of vital records, systems, and equipment, including the ability to access and use such records. Examples of vital records include emergency plans and documents, staffing assignments, and selected program records needed to continue critical operations. Vital records and systems include any IT

applications or systems that are necessary for the Department to perform its minimum essential functions.

Table 4: Format for Identifying Critical Data needs

Critical Service Process	or	Vital Record	Description	Form of Record	Type of Record	Time Critical?

Step 5: Protection of Critical Data

The next step after identification of vital records is determination and selection of protection methods. This necessitates first looking at the current methods of protection and preservation. The routine maintenance program for the records in question may be sufficient for the protection of information in the event of a disruption to critical processes and services. However, the effectiveness of the protection method should always be evaluated in light of continuity concerns. The backup team should take the current backup and retention schedules for each vital record and ask if the files should be backed up more often or retained for greater periods. Replication of data or of a server in an alternate facility or scanning paper records is also recommended. Storing duplicate files off-site, if they are not currently so stored, can also be an option.

Table 5: Format for Protection of critical data

Vital Record	Storage Location	Maintenance Frequency	Current Protection Method(s)	Recommendations for Additional Protection Method(s) (if necessary)

After completion of all the above steps, the final phase of a continuity program is the execution of a continuity plan during an actual disruption. This phase is generally considered during plan development, because all continuity plans should contain strategies for resumption and recovery of operations that include procedures for emergency response; plan activation; communication; evacuation; and data preservation, salvage, and restoration.

If all the steps are planned and implemented properly, it has the potential to thwart any kind of attack, natural or man made from disturbing the schedule of the organization.

Check Your Progress 1

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) Define BCP.

.....
.....
.....
.....

2) What is the four-step approach for developing Business Continuity Program?

.....
.....
.....
.....

3) What is Recovery Time Objective?

.....
.....
.....
.....

4) What is Recovery Point Objective?

.....
.....
.....
.....

1.4 BUSINESS CONTINUITY PROGRAM STAGES

A BCP consists of sequential stages that must be performed in proper order to ensure that the business functions without interruptions and safeguard of business functions are not compromised.

The first such stage is initiation of such a proposal by the management. It is followed by Risk Analysis (RA) and Business Impact Analysis (BIA).

1.4.1 Initiation

The first step is to obtain the commitment of the management and all the stakeholders towards the plan. They have to set down the objectives of the plan, its scope and the policies. An example of a decision on scope would be whether the target is the entire organization or just some divisions, or whether it is only the data processing, or all the organization's services.

Broadly, the objective of the Business Continuity Program (BCP) for a business can only be – to identify and reduce risk exposures and to proactively manage the contingency. The specific objectives that a BCP can set will be described in the subsequent sections.

The final outcome of the BCP exercise is:

- a set of measures to prevent disasters
- a BCP operational team, trained to handle the situation
- a plan that provides a roadmap when disaster strikes – a plan that is sufficient and complete, detailing what needs to be done with each element that falls within the plan's scope.

1.4.2 Risk Assessment

Risk assessment is the exercise of identifying and analyzing the potential vulnerabilities and threats.

The sources of risks could be:

- community-wide hazardous events
- accidents or sabotage causing extreme material disaster
- security threats, network and communication failures
- Disastrous application errors each of these areas should be looked at in the light of the business and the exact possible source located for each source identified.

The magnitude of the risk and the probability of its occurrence must be

evaluated to judge the extent of risk exposure. Risk exposure is the easiest way to know how much attention needs to be paid to a source of risk.

Planning is done for both — prevention and control. Accidents and sabotage can be prevented using measures of physical security and personnel practices. Vulnerability assessment and reviews of existing security measures can throw up areas where access control, software and data security, or backups are required. Application errors can be prevented by effective reviews and testing during the software releases.

The end result of the Risk Assessment should be a risk-benefit analysis statement giving the exact threats, and the estimated exposure together with the contingency and mitigation actions required, and also the benefits arising out of covering the risk. This statement should also delineate any assumptions or constraints that exist.

Often, this exercise will show that the complete physical disaster has a remote probability of occurring and application crashes, or security break-ins are very frequent. However, only having a procedure for handling catastrophic disasters without a plan for application failure or vice versa is not advisable. The solution is to prepare a BCP for the worst-case, i.e., complete destruction of the site providing the services. Any other outage can then be easily tackled using a sub-set of the main plan.

Table 6: Risk Assessment Sheet

Risk Type	Event	Probability of Occurrence
		0.1=low 0.3=medium 0.5=high
Natural	Tornado	
	Hurricane	
	Earthquake	
	Flooding	
	Snow/Ice	
	Temperature Extremes	
Human	Labor Strike	
	Supplier Failure	
	Vandalism/ Theft	
	Terrorism	
	Inadequate Training	

	Bomb Threat	
	Arson	
	Civil Disorder	
Technological	Hardware Failure	
	Software or Application Failures	
	Electrical Outage	
	Telecom Outage	
	Water or Plumbing Outage	
	Toxic Contamination	

1.4.3 Business Impact Analysis

Business Impact Analysis (BIA) is essentially the process of identifying the critical business functions and the losses and effects if these functions are not available.

It involves talking to the key people operating the business functions in order to assess:

In BIA, the impact as well as requirement for recovery angles are analysed for each of the function.

Impact is generally measured based on the following factors:

- Business Impact
- Side Effects
- Affect on the rest of the business by its outage i.e. the operational impact
- The revenue lost due to its outage i.e. the financial impact
- Legal impact
- Customer issues
- Loss of Market share and brand

The measurement of requirement for recovery is based on the following factors:

- Resources and records required to continue the function
- The bare minimum resource requirements
- Resources from external sources
- Other dependent business functions

- Dependence on other business functions
- Dependence on external suppliers/vendors
- Backup needs

Based on these discussions, it will be possible to classify the business functions as:

- Critical functions:** If these business functions are interrupted or unavailable for some time, it can completely jeopardize the business and cause heavy damages to the business.
- Essential functions:** Those functions, whose loss would seriously affect the organization's ability to function for long.
- Necessary functions:** The organization can continue functioning; however, absence of these functions would limit their effectiveness, to a great extent.
- Desirable functions:** These functions would be beneficial; however, their absence would not affect the capability of the organization.

BIA helps define the recovery objectives. In the course of this study, it might be possible to discover that when resuming operations after a disaster, it is enough to recover to a limited capacity, i.e., recover to the extent of handling 40 percent of the usual workload within 24 hours.

Interdependence between various functions both internal and external is crucial information obtained as part of the analysis. While consolidating the information gathered from the questionnaires/discussions and ranking the functions to derive the recovery priority, one must not overlook functions, which by themselves are low priority, however, have some critical functions depending on them. By virtue of this dependence, they also become important.

Cost considerations are also to be taken care of during this exercise. Various costs that must be kept in mind are:

- Revenue losses and opportunity losses will be directly proportional to the time taken for recovery
- Cost of a recovery strategy will be inversely proportional to the time permitted for recovery
- Cost of the possible recovery strategy must be compared with the actual loss due to the outage before accepting the strategy. If the solution proposed costs much more than the projected losses, it will not be possible to justify the investment to the management.

When presenting the findings of the business impact analysis, the results must also be expressed in business terms. Quantifying the impact, possibly in terms of money, will catch the attention of the management. Stating the impact in terms of time will help in proposing concrete recovery goals. Stating the requirements in technical terms will help planning the recovery strategies. Ultimately, the business impact analysis must justify the continuity plan and aid selection of the best possible recovery strategy within the budget.

1.5 BCP GOALS AND STRATEGIES

An effective Business Continuity Program should include strategies on Prevention, Response, Resumption, Recovery and Restoration.

1.5.1 Prevention

Prevention aims at lessening the chances of the disaster happening. Strategies for prevention would include both deterrent and preventive controls.

- Deterrent controls reduce the likelihood of the threats.
- Preventive controls safeguard the vulnerable areas to ward off any threat that occurs and reduce its impact.

Having these measures in place is always more cost-effective than attempting recovery after the interruption. The aim should be to cover as many as possible of the risks identified, using deterrent and preventive controls, so that the recovery strategy has to work only on the residual risks.

A wide variety of such controls exist. Some of the common ones are described below.

- **Security at the premises:** It is a deterrent control and exists in the form of barriers to protect the location and prevent accidental or unauthorized entry. It could also involve manned or technology-driven surveillance at the location.
- **Personnel procedures:** Areas housing the critical resources could be restricted zones where only authorized people are allowed to enter after some means of identification are provided. The means of identification can be varied depending on the technology used for the identification process.
- **Infrastructure-related:** This includes having an appropriate sized UPS, backup power, air conditioning, smoke/fire detectors, fire extinguishers, waterproofing, fire resistant containers for vital records and backups and also monitoring weather forecasts.
- **Software controls:** The most common of these are authentication, access control, anti-virus, encryption, firewall and intrusion detection systems.

- **Storage and recovery related:** Frequent backups. The various mechanisms will be discussed later in this paper. Offsite storage of vital records and backups later contribute to the resumption and recovery process.

Business firms will want to ensure the availability and safety of their assets. Their security policy addresses these objectives and provides guidelines for usage and management of their assets. An outsider with knowledge of the firm's assets, their layout and the risk assessment results can come up with a plan to intrude into the system. Therefore, these controls or security practices must be reviewed from time-to-time and also be tested to see whether they are penetrable by all categories of people, i.e., by people having valid access, by having complete knowledge of the systems or by a complete outsider. Any of them can misuse the access. These reviews always help to strengthen the measures to the benefit of the organization.

1.5.2 Response

Response is the reaction when the event occurs. It must stem further damage, assess the extent of damage, salvage the business entity's reputation by providing appropriate communication to the external world and indicate a possible recovery timeframe.

The first reaction to an interruption would be to inform all the relevant people about the interruption. If it is an impending interruption about which there is a prior warning, then this notification can be done in advance. Timely notification is important, since it may provide an opportunity to stem any further damage. In a situation where there is adequate time to perform a shutdown, a switchover or an evacuation, it may even completely prevent damage. This, however, requires the presence of diagnostic or detective controls. Such controls either continuously scan themselves for a symptom of interruption (network, servers) or collect such information from external sources (natural calamities).

The exact notification procedure must be laid down. It involves clearly documenting who is to be notified, how, by whom, and also the escalation mechanism.

The Response team sets up a notification hierarchy within the BCP team. Here, the initial information is given to first line of people, who in turn, inform the next line of people, and so on. People belonging to this hierarchy will have different roles.

Generally, the following groups would be involved in response team :

- **Management:** would need to be informed of the status. It has the powers to authorize the emergency response and further actions. The management

will also deal with the press, public, customers and shareholders.

- **Damage Assessment Team:** would assess the damage and rate the severity of the interruption.
- **Technical Team:** would serve as the key decision-makers for further activities of the BCP.
- **Operations Team:** would execute the actual operations of the BCP. It is also important to state an alternative for each contact. In case the primary person is not available or traceable, the backup person is to be notified.

The Damage Assessment Team is among the earliest (along with the management) to be notified of the event. They would be required at the site at the earliest to evaluate the extent of the damage inflicted. In case the site itself has been subject to damage, then they should start their work as soon as an entry is allowed.

The assessment should be done against a plan that is closely related to the business continuity priorities. This means that they should be aware of the area in the site and processes that are crucial to the business. This would help them prioritize their examination and also focus adequately on the critical areas.

This team needs to look at the cause of disruption, whether there is scope to stem additional damage, infrastructure and equipment damage, services affected, vital records damaged, what can be salvaged, what needs repair, restoration and replacement, requirements for insurance claims, if applicable etc.

After receiving the input on the severity of damage to facilities and the extent to which the business is inoperable, the Technical Team can work ahead. Some of the questions faced by them are:

- Is it a disaster? Of what degree?
- When will the impact be felt?
- What is the extent of time to repair/resume/restore?
- Where does one begin?

The BCP must have a set of predefined parameters based on the Business Impact Analysis and their continuity goals to evaluate the information available on the damage. These parameters should differentiate between an interruption and a disaster, and also rate the severity of the event.

An optional step in the emergency response is to move to safety all personnel on the premises and alert the police, fire service and hospitals. This is a step required only if the interruption is of the nature of an accident, act of sabotage or natural calamity.

While the Damage Assessment Team and Technical Team are working, the rest of the BCP team is placed on alert for a possible activation of the continuity plan. The type and extent of the disaster declared would indicate which portions of the BCP need to be implemented. Accordingly, the BCP team is notified and resumption activities are started.

1.5.3 Resumption

Resumption shows the effectiveness of response team. It involves resuming only the time-sensitive business processes, either immediately after the interruption or after the declared Mean Time between Failures (MTBF). All operations are not fully recovered.

The focus shifts to the location different from the normal business facility once the BCP has been activated. It is from here that the resumption, and subsequently, the recovery activities are coordinated. This location normally called command centre will have adequate communication facilities, PCs, printers, fax machines and office equipment to support the activities of the team.

The first decision to be taken is – whether the critical operations can be resumed at the normal business site or at an alternate site. In situations when access to the primary site is denied or the site is damaged beyond use, the operations could move to an alternate site.

Alternate sites can be of the following kinds:

- **Cold Site:** A facility that is environmentally conditioned, but devoid of any equipment. It is ready for all the equipment to move in, i.e., it has telephone points, power supply, and UPS facility, among others. It takes a little time to make this site operational. Using a cold site implies that the business entity has contracts with the providers of all the necessary equipment. These contracts are specifically for a business resumption scenario and therefore will have clauses on the time within which the setup will be completed.
- **Hot Site:** It is an alternate facility having workspace for the personnel, fully equipped with all resources and stand-by computer facilities needed to recover and support critical business functions after a disaster. It is a fully equipped site where the BCP team moves in to start work without further delay.
- **Warm Site:** It is a partially equipped hot site and the data is not too old.
- **Mobile Site:** It is a portable site with a smaller configuration. It can be positioned near the primary site, thus saving travel for the key staff.
- **Mirrored Site:** It is identical in all aspects to the primary site, right down

to the information availability. It is equivalent to having a redundant site in normal times and is naturally the most expensive option.

At the alternate site (or primary site, if still usable), the work environment is restored. Communication, networks, and workstations are set up. Contact with the external world can now be resumed. It is possible that an organization might choose to function in the manual mode until the critical IT services can resume.

1.5.4 Recovery

It addresses the startup of less time-sensitive processes. The time duration of this naturally depends on the time taken for resumption of the time-sensitive functions. It could involve starting up these services at an alternate location.

At the site of recovery (either primary or alternative), the operating system is restored on the stand-by system. Necessary applications are restored in the order of their criticality. When the applications to serve the critical functions are restored, data restoration from backup tapes or media obtained from the offsite storage can be initiated.

Data must also be synchronized i.e. to rebuild data accurately to a predetermined point of time before the interruption. The point to which the restoration is done depends on the requirements of the critical services. Business data comes from different sources, each of which must be reconstructed to reach the desired state of data integrity. The synchronized data must be reviewed and validated. This is mandatory because under such disastrous circumstances, it is possible that there is no test environment available and that applications will resume directly in the production environment. It is therefore necessary to have a clear method, strategy or checklist to perform this validation exercise.

Once the data has reached a reliable state, transactions that have been accumulating since the disaster can be processed and all the critical functions can then resume. Gradually, other services of the business can also begin functioning.

Some of the steps described above are not required for certain recovery strategies. The mechanism of the recovery strategy itself is the reason for it. A description of the technical alternatives is covered along with the recovery goals in subsequent sections.

1.5.5 Restoration

It is the process of repairing and restoring the primary site. At the end of this, the business operations are resumed in totality from the original site or a completely new site, in case of a catastrophic disaster.

Even while the recovery team is supporting operations from the alternate site, restoration of the primary site for full functionality is initiated. In case the original building/work area or primary facility is beyond repair, then a new site is restored. It is possible that the team members of the recovery and restoration team are common.

It must be ensured that the site has the necessary infrastructure, equipment, hardware, software and communication facilities. It is necessary to test whether the site is capable of handling full operations. The operational data must then be uploaded at this site and the emergency site gradually dismantled.

Planning for all activities described above will include defining a time span within which they must be executed. This time duration is defined keeping in mind the recovery goals of the organization. The BCP team must remember that if at any point of time, they exceed this planned time, then the contingency must be escalated to the command centre at once, and immediate solutions must be worked out, or else they might miss their recovery targets.

Check Your Progress 2

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) What is the final outcome of BCP exercise?

.....
.....
.....
.....

2) What strategies should include on Prevention for effective Business Continuity Program?

.....
.....
.....
.....

3) Explain Resumption.

.....
.....
.....
.....

1.6 BUILDING DISASTER RECOVERY PLAN

Although building disaster recovery plan is generally part of BCP, some organizations prefer to prepare DRP independent of BCP so as to make BCP more effective.

To build a disaster recovery plan one needs to take into account a number of items unique to disaster recovery. They include:

- What data is vital to my business?
- How long can the data be unavailable?
- How current does the data need to be?
- What is the cost of a disaster to my company?
- What is the cost of my disaster recovery plan?
- Is performance after a disaster a consideration?
- What type of disaster is possible, or even likely, and how long will it affect my system?

One may consider some, or all, of the applications as vital to the operations of the business. If all applications are vital, we need to recover all the data that the systems use. If only some of our applications are vital, we have to determine what data is associated with those applications.

The length of time between the disaster and recovery of your vital applications is a key factor. If the business cannot continue without access to your data, the disaster recovery plan must take this into account.

The time-sensitive nature of your recovered data can be an overriding factor. If the vital application is a high volume, high change application, recovering week-old data may not be acceptable--even hour-old data may be unacceptable. We may need to recover right up to the point of the disaster.

The type of disaster from which we plan to recover can determine where our disaster recovery site is located. If we foresee only fire and water damage to our computer floor, a disaster recovery site in the building next door may be

acceptable. If we are located in an area prone to hurricanes, or earthquakes, for example, a disaster recovery site next door would be pointless.

When we are planning for disaster recovery, we have to consider the cost of being unable to operate your business for a period of time. We have to consider the number of lost transactions and the future loss of business as our customers go elsewhere. Our disaster recovery solution should not be more expensive than the loss from the disaster, unless our business would fail as a result of the outage caused by a disaster.

What is the real cost of your disaster recovery plan? Keeping track of the total cost of your disaster recovery procedures allows us to look at available options and judge the benefits and cost of each.

The disaster recovery plan should include some performance considerations once you have recovered. Unless your disaster site mirrors your production site, you should determine acceptable levels of throughput and transaction times while operating from the disaster recovery site. The length of time it takes to recover your primary site can also determine what your disaster recovery site has to support in the interim.

1.7 ASSESSMENT OF BCP READINESS OF AN ORGANIZATION

Most of the Businesses would like to have BCP in place, so as to meet any eventuality. After all the steps that we have discussed earlier in the unit are over, a readiness check called BCA (Business Continuity Assessment) must be carried out in order to verify that the processes in the business are robust and proper safeguards are in place to see the organization sail through the crisis period successfully.

BCA is a kind of testing activity to BCP. This process can be carried out using a similar questionnaire such as one presented below:

Table 7: Format for Assessment of BCP Readiness of an Organization

#	Business Continuity Assessment	Response		
		Yes	No	Comments
I	Business Continuity Organization			
	Has a BCP coordinator been appointed with the responsibility for Business Continuity Programming?			
	Are selected key employees identified to form part of the Emergency Response Teams to support and implement the BCP at both the corporate and			

#	Business Continuity Assessment	Response		
		Yes	No	Comments
	process level?			
	Have the Emergency Response Teams been briefed on the roles and responsibilities?			
	Have the Emergency Response Teams received formal disaster recovery training?			
II	Business Continuity Program– General			
	Do you have a clearly defined and documented Business Continuity Program approved and signed off by the executive / senior management?			
	Does the Business Continuity Program identify alternate sites in the event of a disaster?			
	Do you have a budget allocated for the BCP? Are the financial and non-financial resources for the BCP regularly evaluated?			
	Does your BCP planning process comply with the current legal and regulatory requirements?			
	Do the service level agreements with vendors clearly state resumption procedures to be adopted in case of an interruption in their services?			
III	Business Continuity Program– Business Impact Analysis			
	Have you identified and documented the mission critical activities, their dependencies and single points of failure?			
	Have you conducted the business impact analysis and risk assessment?			
	Have you identified specific disaster scenarios to be considered for outage and conducted a gap analysis for the existing disaster combat measures?			
III	Business Continuity Program– Recovery Strategies			
	Are the recovery time objectives established for the critical activities and their dependencies?			
	Have you defined and documented the continuity strategies and the associated risks, identifying the minimum resources required for resumption?			
	Are the records prioritized according to their			

#	Business Continuity Assessment	Response		
		Yes	No	Comments
	criticality to the organization? Have adequate procedures been identified for document preservation and restoration?			
	Does the Business Continuity Program include appropriate back up and recovery solutions for information, data and software?			
	Is there adequate security at the alternate site?			
IV	Business Continuity Program– Development			
	Have emergency evacuation procedures been documented and communicated to the employees?			
	Have roles and responsibilities been assigned to appropriate individuals for communicating with the media in the event of a disaster?			
	Have you maintained an up to date contact list for employees, clients, emergency services, vendors, and regulatory authorities etc to be contacted in the event of a disaster?			
V	Business Continuity Program– Testing and Update			
	Has the Business Continuity Program been adequately tested i.e. at least once a year?			
	Is it maintained effectively to reflect the changes in the business?			
	Has the responsibility for the plan maintenance assigned to appropriate individuals?			

If any organization has all the answers as “NO” in any of the five categories, then it will be facing serious risk in case of any eventuality. Generally, it is recommended that all the organizations must go through a similar Business Continuity Assessment to verify whether BCP has been effectively planned and formulated or not. The results of BCA will help BCP to be revised and in turn making business less prone to risk, which is the ultimate objective of the BCP.

1.8 LET US SUM UP

This unit presents the need of Business Continuity Program from a point of view of both the user as well as the management. The BCP, as we have studied here, is a standard methods by which businesses plan how to continue operations even in the times of emergency / uncertainty.

BCP involves many steps, mainly **Business Impact Analysis (BIA)** and **Risk Assessment (RA)**. A general PPRR model is also sometimes used to define BCP cycle.

When the Risk Assessment and Business Impact Analysis phases are over, what stand out are the essentials to keep the business moving. Classification of the business services is available in terms of services that are:

- Critical
- Essential
- Necessary
- Desirable

This classification makes the continuity priorities clear. Goals are generally quantified in terms of RTO and RPO, where **Recovery Time Objective (RTO)** is the maximum permissible outage time and **Recovery Point Objective (RPO)** is the farthest point to which data loss is permitted.

BCP is not an activity that has only positive aspects. Due to adoption of BCP guidelines, the businesses generally compromise on following factors:

- Performance degradation on account of any measures introduced as a part of BCP.
- Risks involved in the case of any measures introduced as a part of BCP.
- Cost of implementing the BCP.

1.9 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

- 1) Business Continuity Program (BCP) is the standard method by which businesses plan for continuing operations in an emergency. BCP involves several steps, which include performing a Business Impact Analysis (BIA) and a Risk Assessment (RA). It is impossible to properly plan for a disaster if the likely impacts of various disruptions on an Organization are unknown.
- 2) The four-step approach for developing Business Continuity Program.
 - a) Identify all functions;
 - b) Identify essential functions;
 - c) Prioritize those functions; and
 - d) Determine essential function resource requirements.

3) Recovery Time Objective

A recovery time objective (RTO) is the period of time within which systems, processes, services, or functions must be recovered after an outage.

4) Recovery Point Objective

A recovery point objective (RPO) is more specific to information systems. It is the amount of data that can be lost measured by a time index. Thus, an RPO of one hour means that the last hour of data before the failure will not be recovered.

Check Your Progress 2

1) The final outcome of the BCP exercise is:

- a set of measures to prevent disasters
- a BCP operational team, trained to handle the situation
- a plan that provides a roadmap when disaster strikes – a plan that is sufficient and complete, detailing what needs to be done with each element that falls within the plan's scope.

2) Prevention aims at lessening the chances of the disaster happening. Strategies for prevention would include both deterrent and preventive controls for effective Business Continuity Program.

- Deterrent controls reduce the likelihood of the threats.
- Preventive controls safeguard the vulnerable areas to ward off any threat that occurs and reduce its impact.

3) Resumption

Resumption shows the effectiveness of response team. It involves resuming only the time-sensitive business processes, either immediately after the interruption or after the declared Mean Time between Failures (MTBF). All operations are not fully recovered.

The focus shifts to the location different from the normal business facility once the BCP has been activated. It is from here that the resumption, and subsequently, the recovery activities are coordinated. This location normally called command centre will have adequate communication facilities, PCs, printers, fax machines and office equipment to support the activities of the team.

The first decision to be taken is – whether the critical operations can be resumed at the normal business site or at an alternate site. In situations

when access to the primary site is denied or the site is damaged beyond use, the operations could move to an alternate site.

4) Restoration

It is the process of repairing and restoring the primary site. At the end of this, the business operations are resumed in totality from the original site or a completely new site, in case of a catastrophic disaster.

Even while the recovery team is supporting operations from the alternate site, restoration of the primary site for full functionality is initiated. In case the original building/work area or primary facility is beyond repair, then a new site is restored. It is possible that the team members of the recovery and restoration team are common.

1.10 SUGGESTED READINGS

- Andrew Hills, The Definitive Handbook of Business Continuity Management, 2nd Edition, John Wiley and Sons, 2007
- <http://www.disasterrecoveryworld.com>
- <http://www.wikihow.com/Create-a-Business-Continuity-Plan>
- Mark Merkow, James Breithaupt ,Information Security: Principles and Practices, Pearson Education
- Stephen Haag, Maeve Cummings, Information Systems Essentials, TMH, 2009

UNIT 2 OVERVIEW OF BUSINESS CONTINUITY MANAGEMENT LIFE CYCLE

Structure

- 2.0 Introduction
- 2.1 Objectives
- 2.2 Business Continuity Planning (BCP): Overview
 - 2.2.1 Objectives of Business Continuity Planning
 - 2.2.2 BCP Factors for Success
 - 2.2.3 Facility Manager's Planning Role in BCP
- 2.3 The Business Continuity Planning Process
 - 2.3.1 Risk Assessment
 - 2.3.2 Recovery Strategy Development
 - 2.3.3 Crisis Management Planning
- 2.4 Planning Considerations
 - 2.4.1 Alternate Workspace Planning
 - 2.4.2 Secondary Data Center Selection
 - 2.4.3 Emergency Plan Components
- 2.5 Disaster Recovery Planning and Audit
 - 2.5.1 Measures
- 2.6 Auditing
 - 2.6.1 Types of Auditors
 - 2.6.2 Methods
 - 2.6.3 Audit Risk
- 2.7 Business Continuity
 - 2.7.1 Elements of Business Continuity
- 2.8 Overview of Business Continuity Management
 - 2.8.1 Business Continuity Life Cycle
 - 2.8.2 BCM Programme Management
 - 2.8.3 Reviewing and Continually Improving Your Business Continuity Management System
 - 2.8.4 Drawback
- 2.9 Let Us Sum Up
- 2.10 Check Your Progress: The Key
- 2.11 Suggested Readings

2.0 INTRODUCTION

Business continuity planning (BCP) is "planning which identifies the organization's exposure to internal and external threats and synthesizes hard

and soft assets to provide effective prevention and recovery for the organization, whilst maintaining competitive advantage and value system integrity”.

2.1 OBJECTIVES

After studying this unit you should be able to:

- understand Business Continuity Planning (BCP);
- understand The Business Continuity Planning Process;
- identify different types of audit; and
- understand Business Continuity Life Cycle.

2.2 BUSINESS CONTINUITY PLANNING (BCP): OVERVIEW

Business entities today exist in a highly competitive world. They are constantly innovating to meet their business objectives of providing essential and unique services to their customers. Technology advances have enabled them to achieve their varied strategies. And yet, the threats of disaster, on account of business interruption, are not extinct – in fact, they have also evolved along with the technology.

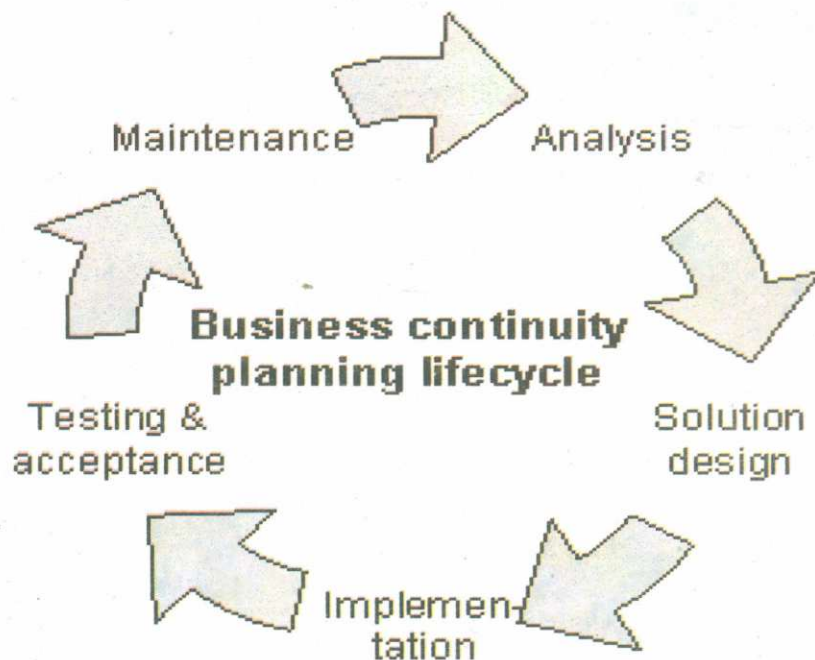


Fig. 1

Business interruption does happen – but what is of significance is, how much of the consequences of such interruptions can the business afford? Business Continuity Planning is the act of proactively working out a way to prevent, if possible and manage the consequences of a disaster, limiting it to the extent that a business can afford. There are various threats and vulnerabilities to which business today is exposed. They could be:

- Catastrophic events such as floods, earthquakes, or acts of terrorism.
- Accidents or sabotage.
- Outages due to an application error, hardware or network failures.

Some of them come unwarned. Most of them never happen. The key is to be prepared and be able to respond to the event when it does happen, so that the organization survives; its losses are minimized; it remains viable and it can be “business as usual”, even before the customers feel the effects of the downtime. An effective Business Continuity Plan serves to secure businesses against financial disasters. The bonus customer satisfaction enhanced corporate image and no dip in the market share.

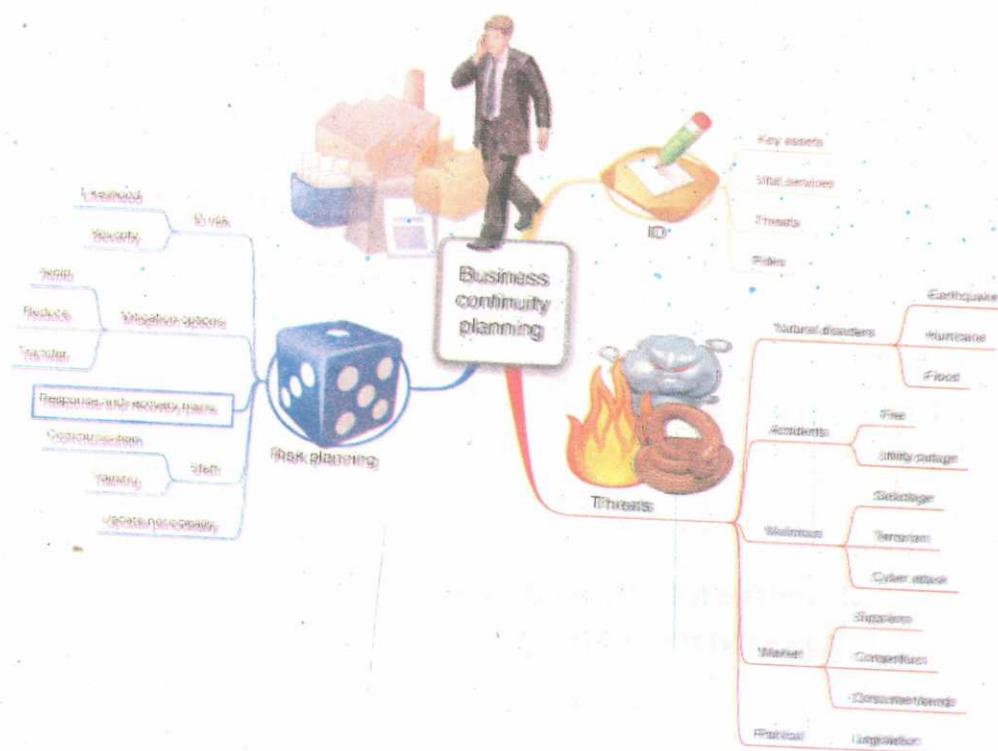


Fig. 2

2.2.1 Objectives of Business Continuity Planning

- Safeguard the Company's Assets
 - People
 - Facilities

- Processes
- Records
- Identify and Mitigate Risks
 - Minimize probability of business interruption
 - Reduce exposure to loss in the event of an interruption
 - Identify impact of outage over time
 - Define recovery objectives to maintain business viability in a disaster
- Resume Critical Functions within a Pre-Defined Timeframe
 - Define incident response, assessment and recovery procedures

BCP Business Drivers

- Understand what drives your business to do this type of planning
 - Legal/regulatory requirement
 - Financial impact from loss of business
 - Loss of customer confidence and/or impact to industry standing
 - Need to address known vulnerabilities or improve operational efficiency
 - Requirement of doing business with some customers and partners
 - Elimination of reliance on ad hoc efforts
 - Employee confidence and retention
- Varies by industry
 - Service industry drivers tend toward customer confidence or legal requirements
 - Production industry drivers tend toward financial loss and operational efficiency

2.2.2 BCP Factors for Success

- BCP program has visible and tangible support from the highest levels of management
- Assign a resource to be a Business Continuity Coordinator
 - Part-time to multiple full-time positions depending on size
- Involve the entire business in the planning process
 - IT cannot do this in a vacuum

- Complete crisis management planning and training early in the implementation process to minimize risk
- Provide training and awareness programs for all employees
 - Message specific to employee's role be realistic about timeline and cost.

2.2.3 Facility Manager's Planning Role in BCP

- Facility Managers play a critical role pre- and post-disaster
 - Pre-disaster
 - Emergency planning and training
 - Coordination with building management
 - Identification of alternate workspace for staff
 - Understanding insurance policy
 - Damage assessment and documentation requirements
 - Insurance adjuster emergency contact information
 - Post-disaster
 - Damage assessment and documentation
 - Salvage operations
 - Facilities restoration/vendor coordination
 - Set up alternate workspace
- Most critical role is to understand the post-disaster needs of the business
 - Know what you are planning for

2.3 THE BUSINESS CONTINUITY PLANNING PROCESS

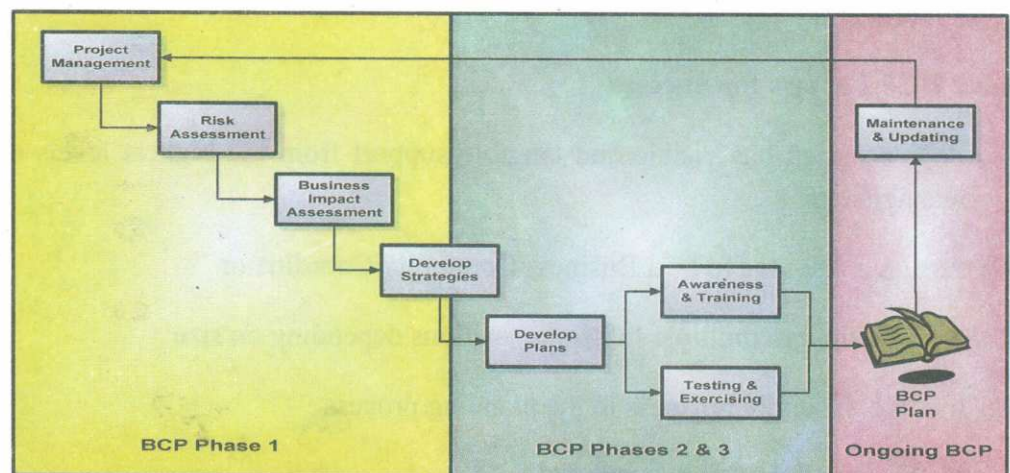


Fig. 3

2.3.1 Risk Assessment

The purpose of the Risk Assessment is to determine the events that can adversely affect the company and its facilities, the damage such events can cause and the controls needed to prevent or minimize loss

Process

- Perform interviews and conduct facility and building walkthroughs to gather data
 - Document organizational structure and critical processes and systems
 - Document components of the critical infrastructure
- Identify single points of failure both with internal and external (vendor/partner) infrastructure and systems
- Identify potential threats, vulnerabilities and impacts
- Determine options and alternatives for controls (mitigations)
- Present a Decision matrix for implementing controls

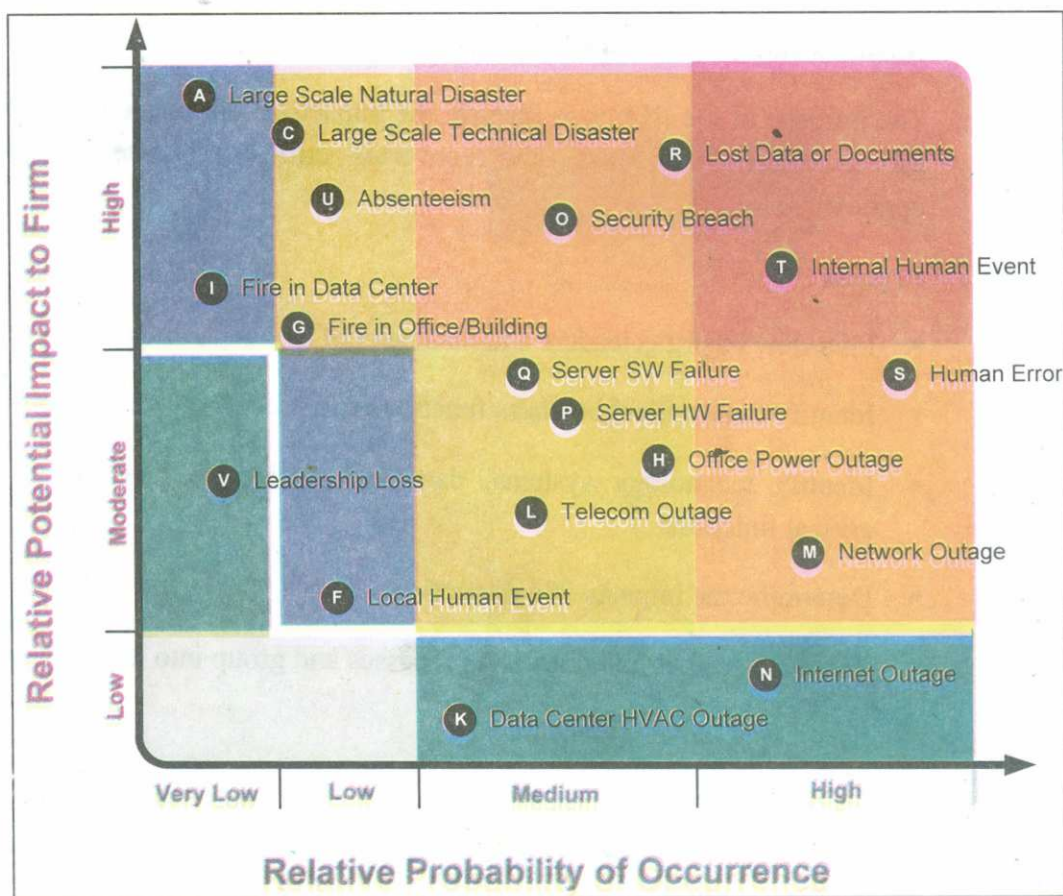


Fig. 4: Sample Impact Chart

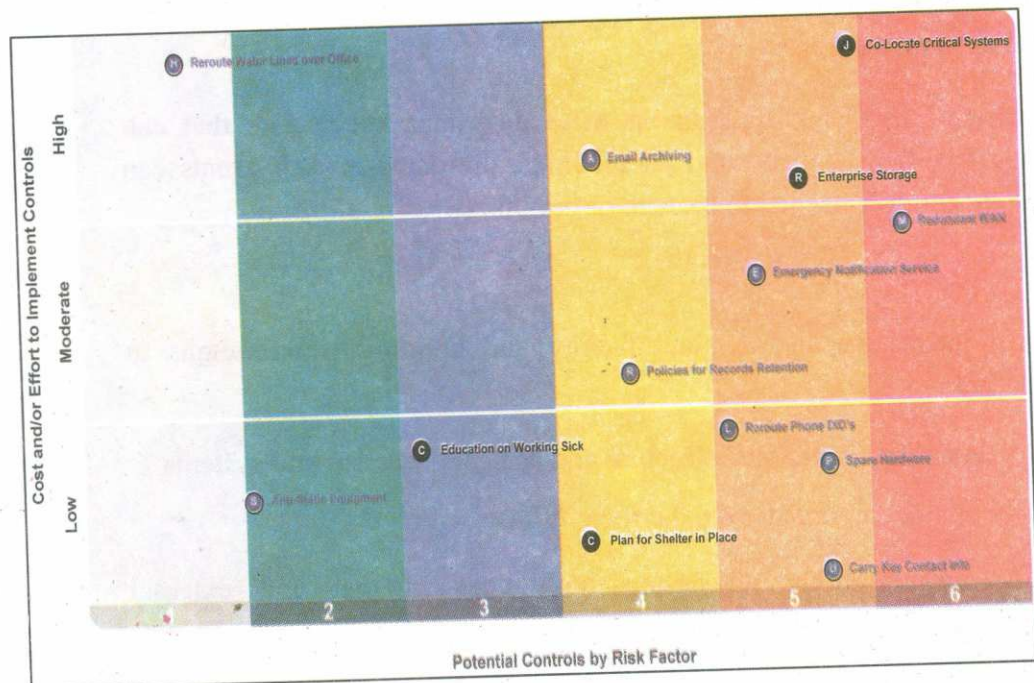


Fig. 5: Sample Risk Mitigation Matrix

- Begin with those items with the highest Risk Factor
- Controls with Low cost/effort to implement are “Low Hanging Fruit” for implementation

Business Impact Assessment (BIA)

The purpose of the BIA is to identify the impacts of an outage on the business and to establish objectives for recovering critical processes, systems and applications

Process

- Interview business leaders and managers of key departments
- Identify time-critical business functions and processes
- Identify technology systems, data and workspace required to support critical functions
- Determine the impacts of a disruption
- Prioritize critical functions and processes and group into levels
- Establish Recovery Objectives
 - Establish levels such as Critical, Essential and Important group functions by level
 - When will we recover and to what level of service?
 - RTO = Recovery Time Objective (tolerance for downtime)
 - RPO = Recovery Point Objective (tolerance for data loss)

2.3.2 Recovery Strategy Development

Recovery strategies outline the approach that will be used to recover critical functions, processes, systems and data in the event of a disruption or disaster

Process

- Validate recovery objectives defined in BIA
- Identify potential strategies for recovering critical functions, systems and applications
- Identify required resources and alternate locations
- Compile costs, advantages and disadvantages
- Compare recovery options and make recommendation to management
- Facility Managers must understand IT needs to ensure proper selection of the secondary data center and alternate worksite facilities

2.3.3 Crisis Management Planning

- Determine structure and format of crisis management team (CMT) and recovery teams
 - Be realistic about how decisions get made
 - Do not establish CMT team structure that is not empowered to make decisions
 - Get the team together to discuss responsibilities
- Determine basic problem escalation process
 - Who calls whom on the CMT
 - When is the whole CMT assembled
 - When are other recovery teams assembled
- Set structure for internal/external communications
 - Who/how/when staff is notified
 - Calling trees
 - Universal voicemail box for status updates
 - Website updates
 - Who/how/when customers or key stakeholders are notified
- Take all critical contact information offsite
 - Every CMT member should have immediate access to this information
 - Include staff, clients, key vendor contact information

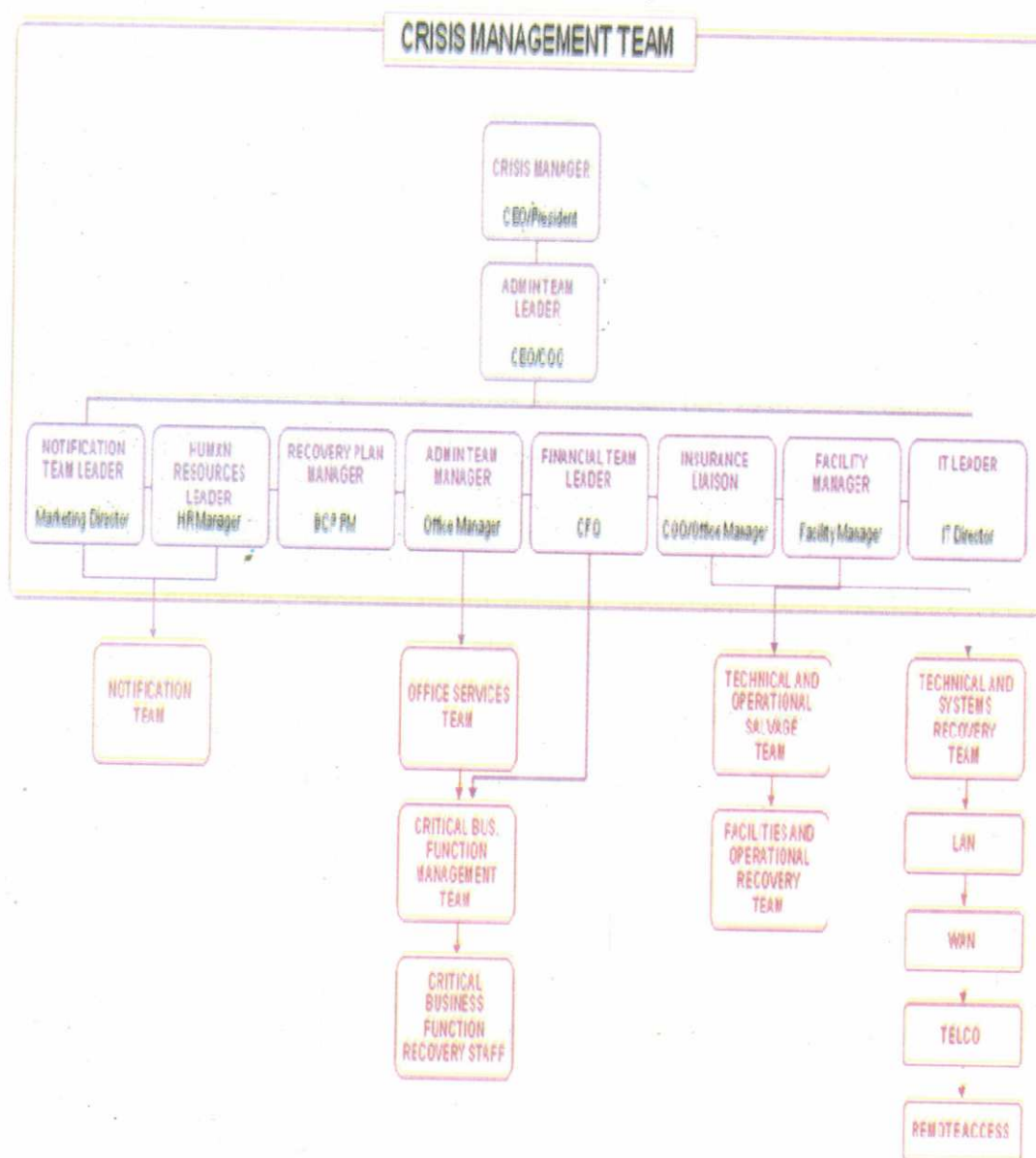


Fig. 6: Crisis Management and Recovery Team Structure

2.4 PLANNING CONSIDERATIONS

2.4.1 Alternate Workspace Planning

- Develop approach to build-out of employee workspace
 - Once you understand what functions are critical to the business, you should have an idea of how many staff will be needed to recover the business
 - If possible, prepare pre-configured equipment and supplies in an offsite location
- Consider the following when identifying alternate workspace

- Geographic considerations
 - Where do critical staff live
 - Distance to primary facility
 - Transportation infrastructure issues (i.e., getting there)
- Space and technology requirements
 - Furniture and desks
 - Equipment (fax, copiers, printers)
 - Power requirements
 - Phones
 - Internet connectivity (pay attention to bandwidth requirements)
- Options for space
 - Other branches/offices
 - Customer locations
 - Hotels (have at least 3 options geographically distributed around town)
 - Some facilities will not guarantee dedicated workspace in a large-scale disaster
 - Some staff work from home

2.4.2 Secondary Data Center Selection

- Build secondary systems in a space geographically distant enough from the primary site that the same disaster will not impact both sites
 - General rule is 50 – 100 miles
 - Really dependant upon location
 - Chicago area does not historically have large-scale disasters
 - Locations like Florida or California potentially require hundreds of miles of geographic separation
- Proximity to existing systems support staff
- Capabilities/Infrastructure of the specific facility - tour and get reviews
- Availability of telecom vendor POP and/or other specialty connectivity
- Power and cooling capabilities to handle high-density equipment
- Availability of additional contiguous space for future growth

	External Hardened Facility	Internal Site
Advantages	• Co-location sites have secondary and sometimes tertiary levels of redundancy in power and telecommunications • Service provider is responsible for tangible facilities maintenance potentially reducing long term costs due to build out of new applications and resulting infrastructure upgrades that may be required • Some service providers can also provide disaster assistance in recovery effort	• Company personnel maintain total control of recovery effort • Company personnel would be onsite to maintain all equipment, monitoring and updates • Annual recurring costs are typically less than a co-location site
Disadvantages	• Ultimately, the Company will be reliant upon an outside vendor to meet its obligations • Annual recurring costs	• Internal site may not have power or telecommunications redundancy • Many office buildings do not allow generators for surviving long-term power outages • Any existing data center would need to be built out impacting start up costs and timeline

Fig. 7: Secondary Data Center Options

2.4.3 Emergency Plan Components

- Emergency planning is usually done collaboratively between building management and facilities managers
- Building management plans generally consist of
 - Evacuation protocols and processes
 - Generally does not include outside assembly point and headcount of employees
 - Fire warden/floor search processes
 - Shelter in place requirements
- Should also consider adding other components
 - Post-evacuation assembly site and headcount of employees
 - Hazardous materials
 - USPS guidelines for mail handling
 - Building shutdown from outside hazmat spill
 - Medical emergencies
 - What to do if you spot a fire
 - Bomb threat
 - Evacuating employees with disabilities
 - Walk-in threats/violence

Check Your Progress 1

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) What is involved in preparing a Business Continuity Management Plan?

.....

.....

.....

.....

2) Explain BIA.

.....

.....

.....

.....

2.5 DISASTER RECOVERY PLANNING AND AUDIT

Disaster recovery as a concept developed in the mid to late 1970s as computer center managers began to recognize the dependence of their organizations on their computer systems. At that time most systems were batch-oriented mainframes which in many cases could be down for a number of days before significant damage would be done to the organization.

Disaster recovery is the process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster. Disaster recovery is a subset of business continuity. While business continuity involves planning for keeping all aspects of a business functioning in the midst of disruptive events, disaster recovery focuses on the IT or technology systems that support business functions.

Disasters can be classified in two broad categories. The first is natural disasters such as floods, hurricanes, tornadoes or earthquakes. While preventing a natural disaster is very difficult, measures such as good planning which includes mitigation measures can help reduce or avoid losses. The second category is man made disasters. These include hazardous material spills, infrastructure failure, or bio-terrorism. In these instances surveillance and mitigation planning are invaluable towards avoiding or lessening losses from these events. Control measures are steps or mechanisms that can reduce or

eliminate various threats for organizations. Different types of measures can be included in BCP/DRP.

2.5.1 Measures

Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking) and other IT infrastructure. A business continuity plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication and reputation protection and should refer to the disaster recovery plan (DRP) for IT related infrastructure recovery / continuity. This article focuses on disaster recovery planning as related to IT infrastructure. Types of measures:

Preventive measures: These controls are aimed at preventing an event from occurring.

Detective measures: These controls are aimed at detecting or discovering unwanted events.

Corrective measures: These controls are aimed at correcting or restoring the system after disaster or event.

These controls should be always documented and tested regularly.

2.6 AUDITING

The general definition of an audit is an evaluation of a person, organization, system, process, enterprise, project or product. The term most commonly refers to audits in accounting, but similar concepts also exist in project management, quality management and energy conservation.

When conducting an audit of a disaster recovery plan the following factors should be considered:

Written disaster recovery plan with continual updating
Designated hot site or cold site
Ability to recover data and systems
Processes for frequent backup of systems and data
Tests and drills of disaster procedures
Data and system backups stored offsite
Appointed disaster recovery committee and chairperson
Visibly listed emergency telephone numbers
Insurance
Procedures allowing effective communication
Updated system and operation documentation
confirmation
Emergency procedures
Backup of key personnel positions
Hardware and software vendor list
Mission statement
Both manual and automated procedures in place
Contractual agreements with external agencies/companies.

Written Disaster Recovery Plan with Continual Updating to be effective the plan must be in writing, must be understandable and must be accessible to

those who need it. Because of constant changes that occur in the modern business environment, a plan should be updated frequently to deal with new and existing threats as they become known. The auditor needs to determine if procedures stated in the plan to achieve these ends are actually used in practice. This can be accomplished through:

1. Direct observation of procedures
2. Examination of the disaster recovery plan
3. Inquiries of personnel
4. Testing of processes for reasonableness and validity

2.6.1 Types of Auditors

Auditors of financial statements can be classified into two categories:

1. External auditor / Statutory auditor is an independent Public accounting firm engaged by the client subject to the audit, to express an opinion on whether the company's financial statements are free of material misstatements, whether due to fraud or error. For publicly-traded companies, external auditors may also be required to express an opinion over the effectiveness of internal controls over financial reporting. External auditors may also be engaged to perform other agreed-upon procedures, related or unrelated to financial statements. Most importantly, external auditors, though engaged and paid by the company being audited, are regarded as independent auditors.

The most used external audit standards are the US GAAS of the American Institute of Certified Public Accountants; and the ISA International Standards on Auditing developed by the International Auditing and Assurance Standards Board of the International Federation of Accountants

Internal auditors are employed by the organization they audit. They perform various audit procedures, primarily related to procedures over the effectiveness of the company's internal controls over financial reporting. Due to the requirement of Section 404 of the Sarbanes Oxley Act of 2002 for management to also assess the effectiveness of their internal controls over financial reporting (as also required of the external auditor), internal auditors are utilized to make this assessment. Though internal auditors are not considered independent of the company they perform audit procedures for, internal auditors of publicly-traded companies are required to report directly to the board of directors, or a sub-committee of the board of directors and not to management, so to reduce the risk that internal auditors will be pressured to produce favorable assessments.

2. Internal Audit: The most used Internal Audit standards are those of the Institute of Internal Auditors. Consultant auditors are external personnel contracted by the firm to perform an audit following the firm's auditing standards. This differs from the external auditor, who follows their own auditing standards. The level of independence is therefore somewhere between

the internal auditor and the external auditor. The consultant auditor may work independently, or as part of the audit team that includes internal auditors. Consultant auditors are used when the firm lacks sufficient expertise to audit certain areas, or simply for staff augmentation when staff are not available. Quality auditors may be consultants or employed by the organization.

2.6.2 Methods

Designated hot site or cold site

A hot/cold site is a location that an organization can move to after a disaster if the current facility is unusable. The difference between the two is that a hot site is fully equipped to resume operations while a cold site does not have that capability. There is also what is referred to as a warm site which has the capability to resume some, but not all operations. The decision a company makes when determining what type of site to establish depends on a cost-benefit analysis and the needs of the individual organization. The plan should also spell out how relocation to a new facility is to be conducted. A company should have occasional tests and conduct trials to verify the viability and effectiveness of the plan and to determine if any deficiencies exist and how they can be dealt with. An audit of a company Disaster Recovery Plan should primarily look into the probability that operations of the organization can be sustained at the level that is assumed in the plan, as well as the ability of the entity to actually establish operations at the site.

The auditor should:

1. Examine and test the procedures involved
2. Conduct outside research relating to Disaster recovery
3. Determine reasonable standards relating to implementation Tour, examine and research the outside facility

Ability to recover data and systems

The continual backing up of data and systems can help minimize the severity of threats. Even so, the plan should also include information on how best to recover any data that has not been copied. Controls and protections should be in place to ensure that data is not damaged, altered, or destroyed during this process. Information technology experts and procedures need to be identified that can accomplish this endeavor. Vendor manuals can also assist in determining how best to proceed.

Processes for frequent backup of systems and data

The auditor should determine if these processes are effective and are actually being implemented by personnel. This can be accomplished through:

1. Direct observation of the processes

2. Analyzing and researching the equipment used
3. Conducting computer assisted audit techniques and tests
4. Examination of paper and paperless records

Tests and drills of disaster procedures

Practice drills should be conducted periodically to determine how effective the plan is and to determine what changes may be necessary. The auditor's primary concern here is verifying that these drills are being conducted properly and that problems uncovered during these drills are addressed and procedures designed to deal with these potential deficiencies are implemented and tested to determine their effectiveness.

Data and system backups stored offsite

The auditor can verify this through paper and paperless documentation and actual physical observation. Testing of the backups and procedures should be done to confirm data integrity and effective processes. The security of the storage site also needs to be confirmed.

Appointed disaster recovery committee and chairperson

The entity needs to appoint individuals responsible for designing and implementing the plan when needed. Generally, this consists of a team headed by a project manager, with a deputy manager who has the capability to take over the responsibilities if needed. The qualities needed for this position vary depending on the organization.

The qualities of the project manager generally include:

1. Good leadership abilities
2. Strong knowledge of company business
3. Strong knowledge of management processes
4. Experience and knowledge in Information technology and security
5. Good project management skills

Other members of the team need to have a clear understanding and ability to perform the needed procedures. An auditor needs to examine and assess the project and deputy project manager's training, experience and abilities as well as to analyze the capabilities of the team members to complete assigned tasks and that more than one individual is trained and capable of doing a particular function. Tests and inquiries of personnel can help achieve this objective.

Visibly listed emergency telephone numbers, the auditor can verify through direct observation that emergency telephone numbers are listed and easily accessible in the event of a disaster.

Insurance

The auditor should determine the adequacy of the company's insurance coverage (particularly property and casualty insurance) through a review of the company's insurance policies and other research. Among the items that the auditor needs to verify are: the scope of the policy (including any stated exclusions), that the amount of coverage is sufficient to cover the organization's needs and that the policy is current and in force. The auditor should also ascertain, through a review of the ratings assigned by independent rating agencies, that the insurance company or companies providing the coverage have the financial viability to cover the losses in the event of a disaster.

Backup of key personnel positions

Clearly written policies and specific communication with employees should be used to substantiate this. There also must be confirmation that the personnel backups can actually do the duties assigned to them in an event of an emergency. Periodic training can also help alleviate this. This training should include updates to existing job positions and testing to confirm proficiency.

The auditor needs to verify that:

1. Policies are being enforced
2. Testing is effective
3. Training is adequate

2.6.3 Audit Risk

Audit risk (also referred to as residual risk) refers to acceptable audit risk, i.e. it indicates the auditor's willingness to accept that the financial statements may be materially misstated after the audit is completed and an unqualified (clean) opinion was issued. If the auditor decides to lower audit risk, it means that he wants to be more certain that the financial statements are not materially misstated.

$$AR = IR * CR * DR$$

where IR is inherent risk, CR is control risk and DR detection risk is the conditional probability that the auditor does not detect a material misstatement in the F/S, given that one exists.

DR is split between two components; SR (Sampling Risk) and NSR (Non-Sampling Risk) SR is the risk that the sample selected by the auditor does not properly reflect the population of the data being sampled. The conclusion drawn from such a sample will therefore not be applicable to the entire population.

NSR is the detection risk other than SR that the auditor will not detect a material misstatement. This could be due to a variety of reasons e.g. human error.

2.7 BUSINESS CONTINUITY

Business continuity is the activity performed by an organization 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.

The foundation of Business Continuity are the standards, program development and supporting policies; guidelines and procedures needed to ensure a firm to continue without stoppage, irrespective of the adverse circumstances or events. All system design, implementation, support and maintenance must be based on this foundation in order to have any hope of achieving Business Continuity, Disaster Recovery, or in some cases, system support. Business continuity is sometimes confused with disaster recovery, but they are separate entities. Disaster recovery is a small subset of business continuity. It is also sometimes confused with Work Area Recovery (due to loss of the physical building which the business is conducted within); which is but a part of business continuity.

The term Business Continuity describes a mentality or methodology of conducting day-to-day business, whereas Business Continuity Planning is an activity of determining what that methodology should be. The Business Continuity Plan may be thought of as the incarnation of a methodology that is followed by everyone in an organization on a daily basis to ensure normal operations.



Fig. 8

- Establish a focal point with clear responsibilities for business continuity Planning.
- Identify and formulated Document in a business continuity plan the Center's disaster Recovery and responsibilities.
- Include in the business continuity plan how damage will be assessed.
- Clearly document authority levels and circumstances for Activation / Implement Continuity plan
- Periodically test, review and update as necessary business continuity plans.
- Consider automating the preparation and maintenance of business continuity plans

Some of them come unwarned. Most of them never happen. The key is to be prepared and be able to respond to the event when it does happen, so that the organization survives; its losses are minimized; it remains viable and it can be "business as usual", even before the customers feel the effects of the downtime. An effective Business Continuity Plan serves to secure businesses against financial disasters. The bonus customer satisfaction enhanced corporate image and no dip in the market share.

2.7.1 Elements of Business Continuity

Initiation

The first step is to obtain the commitment of the management and all the stakeholders towards the plan. They have to set down the objectives of the plan, its scope and the policies. An example of a decision on scope would be whether the target is the entire organization or just some divisions, or whether it is only the data processing, or all the organization's services. Management provides sponsorship in terms of finance and manpower. They need to weigh potential business losses versus the annual cost of creating and maintaining the Business Continuity Planning. For this, they will have to find answers to questions such as how much it would cost or how much would be considered adequate. Broadly, the objective of the Business Continuity Planning (BCP) for a business can only be to identify and reduce risk exposures and to proactively manage the contingency.

The specific objectives that a BCP can set will be described in the subsequent sections. The final outcome of the BCP exercise is:

1. a set of measures to prevent disasters
2. a BCP operational team, trained to handle the situation

3. a plan that provides a roadmap when disaster strikes – a plan that is sufficient and complete, detailing what needs to be done with each element that falls within the plan's scope.

The discussions that follow are mainly in the context of IT services provided by an organization. They do not deal with the safety management of the firm's personnel, in case of a disaster.

Risk Assessment

Risk assessment is the exercise of identifying and analyzing the potential vulnerabilities and threats. The sources of risks could be:

1. community-wide hazardous events
2. Accidents or sabotage causing extreme material disaster
3. Security threats, network and communication failures
4. Disastrous application errors

Each of these areas should be looked at in the light of the business and the exact possible source located. For each source identified:

1. the magnitude of the risk and
2. the probability of its occurrence must be evaluated to judge the extent of risk exposure. Risk exposure is the easiest way to know how much attention needs to be paid to a source of risk.

Planning is done for both prevention and control. Accidents and sabotage can be prevented using measures of physical security and personnel practices. Vulnerability assessment and reviews of existing security measures can throw up areas where access control, software and data security, or backups are required. Application errors can be prevented by effective reviews and testing during the software releases. If needed, the expertise of external agencies can easily be called upon to analyze, devise and put in place some of the preventive measures. The tougher part is to come up with activities for controlling the effects of disaster and this necessitates a detailed business impact analysis. The end result of the Risk Assessment should be a risk-benefit analysis statement giving the exact threats and the estimated exposure together with the contingency and mitigation actions required and also the benefits arising out of covering the risk. This statement should also delineate any assumptions or constraints that exist. Often, this exercise will show that the complete physical disaster has a remote probability of occurring and application crashes, or security break-ins are very frequent. However, only having a procedure for handling catastrophic disasters without a plan for application failure or vice versa is not advisable. The solution is to prepare a BCP for the worst-case, i.e., complete destruction of the site providing the services. Any other outage can then be easily tackled using a sub-set of the main plan.

Business Impact Analysis

Business Impact Analysis (BIA) is essentially the process of identifying the critical business functions and the losses and effects if these functions are not available. It involves talking to the key people operating the business functions as:

- a) **Critical functions:** If these business functions are interrupted or unavailable for some time, it can completely jeopardize the business and cause heavy damages to the business.
- b) **Essential functions:** Those functions, whose loss would seriously affect the organization's ability to function for long.
- c) **Necessary functions:** The organization can continue functioning; however, absence of these functions would limit their effectiveness, to a great extent.
- d) **Desirable functions:** These functions would be beneficial; however, their absence would not affect the capability of the organization.

Based on their recovery needs, organizations can come up with standard recovery time frames for the above classifications. For example, Critical functions: < 1 day, Essential functions: 2 -4 days, Necessary functions: 5 -7 days and Desirable functions: > 10 days.

This impact analysis helps to rank the business functions and come up with an order in which they should be brought up. In other words, it defines recovery priorities.

BIA helps define the recovery objectives. In the course of this study, it might be possible to discover that when resuming operations after a disaster, it is enough to recover to a limited capacity, i.e., recover to the extent of handling 40 percent of the usual workload within 24 hours.

It will also be possible to define in detail the resource requirements for making a business function operational after disaster or interruption. This will include infrastructure, manpower, documents, records, machines, phones, fax machines, whatever is needed – with complete specifications. Having adequate details is important, since in the event of disasters, there is bound to be some amount of panic and it may not be possible to come down to such details.

The team and managers actually involved in the day -to-day operations of the business functions would be the best people to talk to during the impact analysis, as they would certainly know the details of the functions. Moreover, they can perform a brainstorming exercise on how an outage of their function would affect the revenue objectives, market position and customer expectations, or how they could restore normal operations, or what resources they would require to operate in normal mode.

Interdependence between various functions (internal and external) is crucial information obtained as part of the analysis. While consolidating the information gathered from the questionnaires/discussions and ranking the functions to derive the recovery priority, one must not overlook functions, which by themselves are low priority, however, have some critical functions depending on them. By virtue of this dependence, they also become important.

Cost considerations are not to be ignored during this exercise. Things to be kept in mind are:

1. Revenue losses and opportunity losses will be directly proportional to the time taken for recovery.
2. Cost of a recovery strategy will be inversely proportional to the time permitted for recovery.
3. Cost of the possible recovery strategy must be compared with the actual loss due to the outage before accepting the strategy. If the solution proposed costs much more than the projected losses, it will not be possible to justify the investment to the management.

When presenting the findings of the business impact analysis, the results must also be expressed in business terms. Quantifying the impact, possibly in terms of money, will catch the attention of the management. Stating the impact in terms of time will help in proposing concrete recovery goals. Stating the requirements in technical terms will help planning the recovery strategies. Ultimately, the business impact analysis must justify the continuity plan and aid selection of the best possible recovery strategy within the budget.

Strategies

Business Continuity Planning should include strategies on:

1. Prevention
2. Response
3. Resumption
4. Recovery
5. Restoration

Prevention aims at lessening the chances of the disaster happening.

Response is the reaction when the event occurs. It must stem further damage, assess the extent of damage, salvage the business entity's reputation by providing appropriate communication to the external world and indicate a possible recovery timeframe. Resumption involves resuming only the time-sensitive business processes, either immediately after the interruption or after the declared Mean Time Between Failures (MTBF). All operations are not

fully recovered. Recovery addresses the startup of less time-sensitive processes. The time duration of this naturally depends on the time taken for resumption of the time-sensitive functions.

It could involve starting up these services at an alternate location. Restoration is the process of repairing and restoring the primary site. At the end of this, the business operations are resumed in totality from the original site or a completely new site, in case of a catastrophic disaster.

Prevention

Strategies for prevention would include both deterrent and preventive controls.

1. Deterrent controls reduce the likelihood of the threats.
2. Preventive controls safeguard the vulnerable areas to ward off any threat that occurs and reduce its impact.

Having these measures in place is always more cost-effective than attempting recovery after the interruption. The aim should be to cover as many as possible of the risks identified, using deterrent and preventive controls, so that the recovery strategy has to work only on the residual risks.

A wide variety of such controls exist. Some of the common ones are described below.

- (a) **Security at the premises:** It is a deterrent control and exists in the form of barriers to protect the location and prevent accidental or unauthorized entry. It could also involve manned or technology-driven surveillance at the location.
- (b) **Personnel procedures:** Areas housing the critical resources could be restricted zones where only authorized people are allowed to enter after some means of identification are provided. The means of identification can be varied depending on the technology used for the identification process.
- (c) **Infrastructure-related:** This includes having an appropriate sized UPS, backup power, air conditioning, smoke/fire detectors, fire extinguishers, waterproofing, fire resistant containers for vital records and backups and also monitoring weather forecasts.
- (d) **Software controls:** The most common of these are authentication, access control, anti-virus, encryption, firewall and intrusion detection systems.
- (e) **Storage and recovery related:** Frequent backups. The various mechanisms will be discussed later in this paper. Offsite storage of vital records and backups or contribute to the resumption and recovery process.

The above list distinctly highlights one aspect: most of the safeguards are closely related to the security policy and practices in an organization.

Business firms will want to ensure the availability and safety of their assets (which includes information). Their security policy addresses these objectives and provides guidelines for usage and management of their assets. Armed with knowledge of the firm's assets, their layout and the risk assessment results, the firm can come up with the necessary controls needed to implement the security policy. These controls or security practices must be reviewed from time-to-time and also be tested to see whether they are penetrable by all categories of people, i.e., by people having valid access, by having complete knowledge of the systems or by a complete outsider. Any of them can misuse the access. The reviews will help enrich or strengthen the measures.

Having a security policy, putting preventive safeguards in place, monitoring the system for intrusions and ensuring action against those who violate it, is itself a deterrent control. Planning for prevention is an exercise that must be done carefully. It has to ensure that the mechanisms used are neither very restrictive, nor would they constitute a bottleneck, nor cause an availability problem, nor allow undesirable/easy access and usage.

Response

The first reaction to an interruption would be to inform all the relevant people about the interruption. If it is an impending interruption about which there is a prior warning, then this notification can be done in advance. Timely notification is important, since it may provide an opportunity to stem any further damage. In a situation where there is adequate time to perform a shutdown, a switchover or an evacuation, it may even completely prevent damage. This, however, requires the presence of diagnostic or detective controls. Such controls either continuously scan themselves for a symptom of interruption (network, servers) or collect such information from external sources (natural calamities).

The exact notification procedure must be laid down. It involves clearly documenting who is to be notified, how, by whom and also the escalation mechanism. A notification call tree within the BCP team is set up. Here, the initial notification is sent to a set of people, who in turn, inform the next set of people and so on. People belonging to this call tree have different roles. The type of information and amount of detail provided as a part of the notification depends on the role of the person. The following groups would be involved:

1. **Management:** would need to be informed of the status. It has the powers to authorize the emergency response and further actions. The management will also deal with the press, public, customers and shareholders.
2. **Damage Assessment Team:** would assess the damage and rate the severity of the interruption.

3. **Technical Team:** would serve as the key decision-makers for further activities of the BCP.
4. **Operations Team:** would execute the actual operations of the BCP.

It is also important to state an alternative for each contact. In case the primary person is not available or traceable, the backup person is to be notified. Notification can be done using various tools: pager, SMS, phone and email. The team is equipped appropriately.

The Damage Assessment Team is among the earliest (along with the management) to be notified of the event. They would be required at the site at the earliest to evaluate the extent of the damage inflicted. In case the site itself has been subject to damage, then they should start their work as soon as an entry is allowed. (Of course, if the calamity is as great as on September 11th 2001, then it is obvious that it is a disaster of the greatest severity.)

The assessment should be done against a plan that is closely related to the business continuity priorities. This means that they should be aware of the area in the site and processes that are crucial to the business. This would help them prioritize their examination and also focus adequately on the critical areas. This team needs to look at:

1. the cause of disruption
2. whether there is scope to stem additional damage
3. infrastructure and equipment damage
4. services affected
5. vital records damaged
6. what can be salvaged
7. what needs repair, restoration and replacement
8. requirements for insurance claims, if applicable Armed with this input (provided by the Damage Assessment Team) on the severity of damage to facilities and the extent to which the business is inoperable, the Technical

Team can work ahead. Some of the questions faced by them are:

1. Is it a disaster? Of what degree?
2. When will the impact be felt?
3. What is the extent of time to repair/resume/restore?
4. Where does one begin?

The BCP must have a set of predefined parameters based on the Business Impact Analysis and their continuity goals to evaluate the information available on the damage. These parameters should differentiate between an interruption

and a disaster and also rate the severity of the event. What the Technical Team uses here is a decision support mechanism based on these parameters before they declare a disaster (of any appropriate scale).

While the Damage Assessment Team and Technical Team are working, the rest of the BCP team is placed on alert for a possible activation of the continuity plan. The type and extent of the disaster declared would indicate which portions of the BCP need to be implemented. Accordingly, the BCP team is notified and resumption activities are started.

An optional step in the emergency response (the first action, in fact) is to move to safety all personnel on the premises and alert the police, fire service and hospitals. This is a step required only if the interruption is of the nature of an accident, act of sabotage or natural calamity.

Resumption

The focus shifts to the command centre once the BCP has been activated. This is a location different from the normal business facility. It is from here that the resumption and subsequently, the recovery activities, are coordinated. The centre will have adequate communication facilities, PCs, printers, fax machines and office equipment to support the activities of the team.

The first decision to be taken is whether the critical operations can be resumed at the normal business site or at an alternate site. In situations when access to the primary site is denied or the site is damaged beyond use, the operations could move to an alternate site.

Alternate sites can be of the following kinds:

- (a) **Cold Site:** A facility that is environmentally conditioned, but devoid of any equipment. It is ready for all the equipment to move in, i.e., it has telephone points, power supply and UPS facility, among others. It takes a little time to make this site operational. Using a cold site implies that the business entity has contracts with the providers of all the necessary equipment. These contracts are specifically for a business resumption scenario and therefore will have clauses on the time within which the setup will be completed.
- (b) **Hot Site:** It is an alternate facility having workspace for the personnel, fully equipped with all resources and stand-by computer facilities needed to recover and support critical business functions after a disaster. It is a fully equipped site where the BCP team moves in to start work without further delay.
- (c) **Warm site:** It is a partially equipped hot site and the data is not too old.
- (d) **Mobile site:** It is a portable site with a smaller configuration. It can be positioned near the primary site, thus saving travel for the key staff.

- (e) **Mirrored Site:** It is identical in all aspects to the primary site, right down to the information availability. It is equivalent to having a redundant site in normal times and is naturally the most expensive option.

At the alternate site (or primary site, if still usable), the work environment is restored. Communication, networks and workstations are set up. Contact with the external world can now be resumed. It is possible that an organization might choose to function in the manual mode until the critical IT services can resume. If the recovery alternative (described in a later section) permits, the critical functions can also be resumed in the automated mode very quickly.

Recovery

At the site of recovery (either primary or alternative), the operating system is restored on the stand-by system. Necessary applications are restored in the order of their criticality. When the applications to serve the critical functions are restored, data restoration from backup tapes or media obtained from the offsite storage can be initiated.

Data must also be synchronized i.e., to rebuild data accurately to a predetermined point of time before the interruption. The point to which the restoration is done depends on the requirements of the critical services. Business data comes from different sources, each of which must be reconstructed to reach the desired state of data integrity. The synchronized data must be reviewed and validated. This is mandatory because under such disastrous circumstances, it is possible that there is no test environment available and that applications will resume directly in the production environment. It is therefore necessary to have a clear method, strategy or checklist to perform this validation exercise.

Once the data has reached a reliable state, transactions that have been accumulating since the disaster can be processed and all the critical functions can then resume.

Gradually, other services of the business can also begin functioning. Some of the steps described above are not required for certain recovery strategies. The mechanism of the recovery strategy itself is the reason for it. A description of the technical alternatives is covered along with the recovery goals in subsequent sections.

Restoration

Even while the recovery team is supporting operations from the alternate site, restoration of the primary site for full functionality is initiated. In case the original building/work area or primary facility is beyond repair, then a new site is restored. It is possible that the team members of the recovery and restoration team are common.

It must be ensured that the site has the necessary infrastructure, equipment, hardware, software and communication facilities. It is necessary to test whether the site is capable of handling full operations. The operational data must then be uploaded at this site and the emergency site gradually dismantled.

Planning for all activities described above will include defining a time span within which they must be executed. This time duration is defined keeping in mind the recovery goals of the organization. The BCP team must remember that if at any point of time, they exceed this planned time, then the contingency must be escalated to the command centre at once and immediate solutions must be worked out, or else they might miss their recovery targets.

Goals

At the end of the phase of Risk Assessment and Business Impact Analysis, what stand out are the essentials to keep the business moving. Classification of the business services is available in terms of services that are:

1. critical
2. essential
3. necessary
4. desirable

This makes the Continuity Priorities clear. Goals can now be quantified in terms of:

1. Recovery Time Objective (RTO): maximum permissible outage time
2. Recovery Point Objective (RPO): the furthest point to which data loss is Permitted.
3. Performance degradation on account of any measures introduced as a part of BCP.
4. Risks involved in the case of any measures introduced as a part of BCP
5. Cost of implementing the BCP

These will drive the operational details of the BCP.

2.8 OVERVIEW OF BUSINESS CONTINUITY MANAGEMENT

“Business Continuity Management (BCM) is a holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities.”

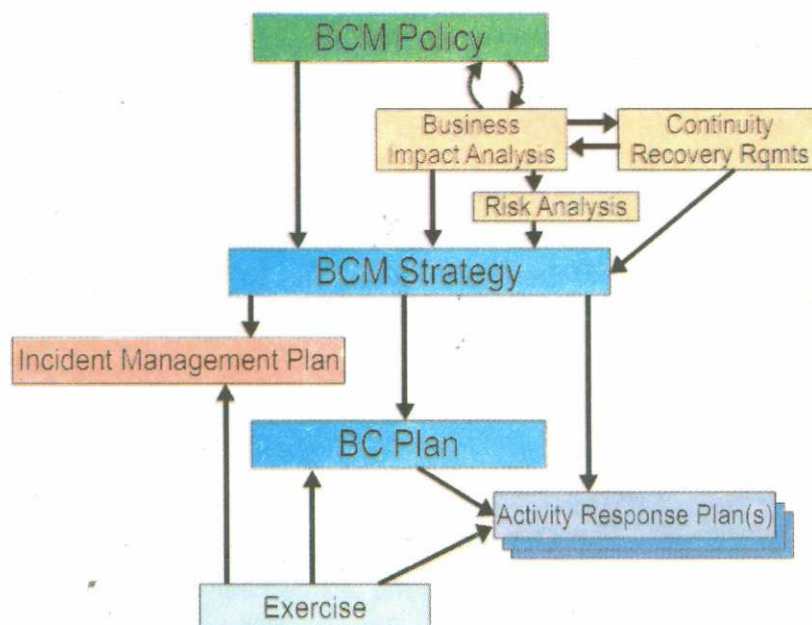


Fig. 9: BCM is a Top-Down Process

2.8.1 Business Continuity Life Cycle

The BCM Life Cycle

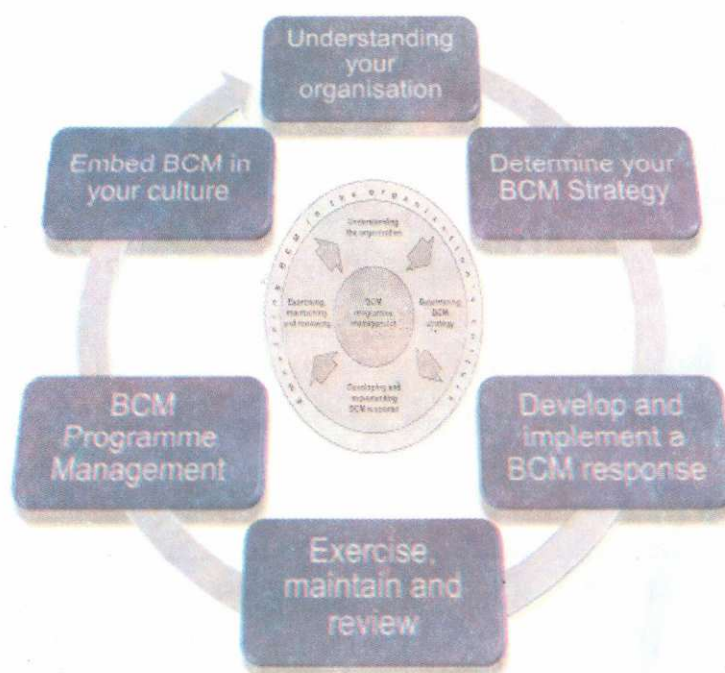


Fig. 10

Business Continuity Management (BCM) is a continuous process and encompasses six distinct steps:

1. BCM programme management

2. Understanding the organization
3. Determining BCM strategies
4. Developing and implementing a BCM response Exercising, maintenance and Review.
5. Embedding BCM in the organization's culture.

Ascure's BCM Services have been designed to match with these steps (one or more BCM Services for each BCM step), hereby assuring compliance to the most recent BCM standards and good practices.

2.8.2 BCM Programme Management

Within this BCM step, Ascure is offering following services:

1. BCM Conceptual design and architecture
2. BCM Programme management

The aim of BCM programme management is to build and maintain a BC capability appropriate to the size and complexity of the organization.

Within the BCM Conceptual design and architecture service, Ascure will provide highly experienced and certified experts to help you design and structure this type of BCM programme that fits best with your organization, BCM ambition and objectives.

Within the BCM Programme management service, Ascure will drive and steer the implementation and roll-out the selected BCM programme in the organization. This includes project and budget control, BCM policy development and the set up of a BCM Framework.

Determining BCM Strategies

Within this BCM Step, Ascure is offering following service:

BCM Strategy Development

The aim of the BCM Strategy development service is to facilitate the decision making process (based upon the information from the RA and BIA and cost/benefit considerations) towards defining a fit-for-purpose response capability, covering people, premises, technology, information, 3rd parties/suppliers.

Developing and Implementing a BCM Response

Within this BCM Step, Ascure is offering following services:

1. Emergency Response and Crisis Management
2. Plans (Response, Recovery, Continuity)

3. Arrangements (Business Continuity Service Level Agreements with 3rd parties).
4. Solutions (Vendor selection, Solution evaluation)

The aim of the BCM Response services is to develop and implement an appropriate response competence (ability to execute plans and actions) and capability (use of alternative infrastructure and technology to support the response).

Embedding BCM in the Organization's Culture

Within this BCM Step, Assure is offering following service:

1. BCM Training and Awareness

The aim of BCM embedding is to ensure that Business Continuity becomes part of the way an organization is managed. Within the BCM training and awareness service, Assure will develop in collaboration with the organization specific training and awareness initiatives in support of the BC Programme.

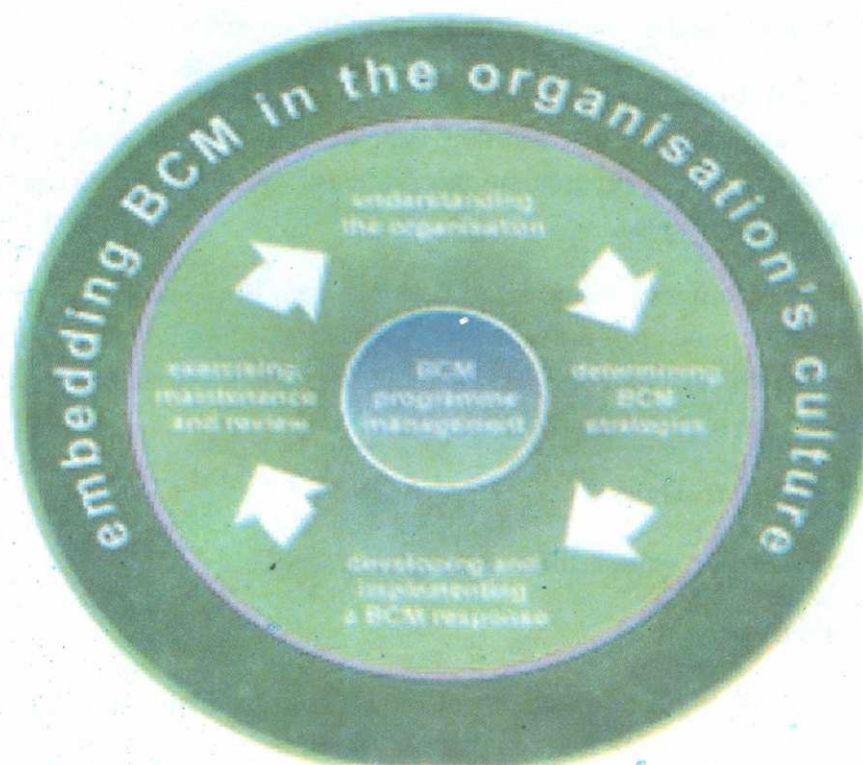


Fig. 11

Furthermore Assure is collaborating very closely with the BCM Academy (BCM A) for the delivery of open class trainings, covering:

1. BCM Essentials
2. BCM Foundation
3. Certified BCM Manager Crisis Management and Communication

What events might you need to deal with?

System failure and how you can continue to do business Facing the media in a crisis– what messages do you want to get across Identify theft – not just individual but whole company theft Physical incidents – Fire, flood and storm damage Reputation – bringing your business into disrepute or even just getting it wrong can lose you customers Fraud – in times of recession statistics show more fraud is perpetrated

Terrorism – How real is the threat?

Recovery – getting your organization back up and running in the shortest time.

2.8.3 Reviewing and Continually Improving Your Business Continuity Management System

The drivers to undertake a BCM programme Legislation, the civil contingences act requires level 1 responders (emergency services, local government) to have in place measures to deal with incidents. As a supplier you might also need to play your part in incident management and therefore need to consider BCM.

Revenues, market share, image and reputation can all be affected if you respond badly. There is significant evidence to suggest that a high proportion (up to 80%) of businesses that are affected by a major incident never recover. Be prepared to stand a greater chance of surviving. Supply chain, can your suppliers provide you with their product or service if there is a problem, will it cause you to fail as your link in the supply chain for your customers?

Insurance, as they say the value of your business can go up or down, Insurance only mitigates to a certain extent and for specific risks. Have you discussed with your insurance company your levels of resilience? As noted above, they are looking for resilience. Good BCM systems and resilience could mean lower premiums.

2.8.4 Drawback

1. It is not for the faint-hearted (the standard is very exacting) and will require time and effort to put in place.
2. You need to consider not just what you do as a business but what others do around you and how that might affect you.
3. Everyone in the business needs to be involved, knowing what to do, where to find information etc in any given situation.
4. The terminology can be new and need explaining in the organization.

Check Your Progress 2

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) What is Business Continuity Management?

.....

.....

.....

.....

2) What is a Business Continuity Management Plan?

.....

.....

.....

.....

3) Why should I prepare a Business Continuity Management Plan?

.....

.....

.....

.....

4) How long will it take to prepare a Business Continuity Management Plan?

.....

.....

.....

.....

2.9 LET US SUM UP

This unit is an effort towards answering some of the fundamental queries about Business Continuity Management Life Cycle. Here in this unit we have done an attempt to provide knowledge to our learners regarding Business Continuity Planning (BCP) and Business Continuity Planning Process. We have also covered the topics like audit and its types.

Check Your Progress 1

- 1) There are just a few steps involved in preparing a Business Continuity Management Plan.
 1. Know your risks.
 2. Conducting a Business Impact Analysis. This involves identifying your key products and services, deciding how long you can stop delivering them and identifying your critical inputs.
 3. Developing continuity strategies to operate your business.
 4. Identifying communications needs.
 5. Being ready to go.
 6. Reviewing your plan.

2) Business Impact Assessment (BIA)

The purpose of the BIA is to identify the impacts of an outage on the business and to establish objectives for recovering critical processes, systems and applications

Process:

- Interview business leaders and managers of key departments
- Identify time-critical business functions and processes
- Identify technology systems, data and workspace required to support critical functions
- Determine the impacts of a disruption
- Prioritize critical functions and processes and group into levels
- Establish Recovery Objectives
 - Establish levels such as Critical, Essential and Important group functions by level
 - When will we recover and to what level of service?
 - RTO = Recovery Time Objective (tolerance for downtime)
 - RPO = Recovery Point Objective (tolerance for data loss)

Check Your Progress 2

1) Business Continuity Management

Business Continuity Management is about being prepared to manage any disruption to your business to ensure the continuity of services to your

customers. You want your customers to know that you can provide “business as usual” even if others around you are experiencing difficulties. The disruption to your business could be caused by an emergency such as a flood, or a critical input disruption such as an extended electricity blackout.

2) Business Continuity Management Plan

A Business Continuity Management Plan comprises those documented arrangements that enable you to manage any disruption to your business and maintain the continuity of services to your customers.

- 3) By preparing a Business Continuity Management Plan your business will be more likely to survive an emergency or critical input disruption. The ability to continue trading while competitors experience disruptions may enable you to gain market share and grow your business. Your staff, key customers and insurer may also like to know you have a Business Continuity Management Plan. This will give them more confidence that your business is well organised and able to withstand business disruptions. Business Continuity Management planning will also help you to better understand your business and its vulnerability.

Businesses are at risk from many natural and societal hazards. These hazards include:

- Bushfires
- Pandemic Influenza
- Floods
- Building fire
- Criminal activity
- Staff loss
- Electrical failure
- Fuel supply disruption
- Machinery failure
- Computer failure

Through adequate preparation, the risks to your business can be minimized.

- 4) The time it takes to develop a Business Continuity Management Plan will depend on the size and complexity of your business. However, for a small business this may only take a few hours. This Guide will lead you through a series of simple steps and questions that will assist you to develop your Business Continuity Management Plan.

2.11 SUGGESTED READINGS

1. Barnes, James C. *A Guide to Business Continuity Planning*. New York, NY: Wiley, 2001.
2. Business Continuity, enterprise BC plan Steve McKinty, Sun Microsystems 31st May 2009, San Francisco, California, USA.
3. "Business Continuity Management" by Hamilton Beazley.
4. Business Continuity Management" by IF4IT.
5. Business Continuity Management John Wiley and Sons, 2010 Business and Economics.
6. BUSINESS CONTINUITY MANAGEMENT by Michael Gallagher
7. ""Business Continuity Management" by Michael Blyth.
8. Business Continuity Planning - A safety net for businesses
9. Business Continuity Planning Methodology by Akhtar Syed, Ph.D., CISSP and Afsar.
10. "Garvey, Martin J. "From Good to Great (Maybe)." *Information-Week*, 3 January 2005.
11. Gerson, Vicki. "Better Safe Than Sorry." *Bank Systems and Technology* 42, no. 1 (2005).
12. Hanna, Greg. "How to Take a Computer Disaster in Stride." *Strategic Finance* 86, no. 7 (2005).
13. Hofmann, Mark A. "Y2K Spurred Continuity Plan That Was Put to Test by 9/11." *Business Insurance* 39, no. 16 (2005).
14. Hoge, John. "Business Continuity Planning Must Extend to Vendors." *Bank Technology News* 18, no. 2 (2005).
15. Hood, Sarah B. "Always Be Prepared." *Canadian Business* 78, no. 6 (2005).
16. Huber, Nick. "Business Continuity Plans Eat 35% of Clearing House's Core IT Spend." *Computer Weekly*, 8 February 2005.
17. Roberts, John and Frank J. Ohlhorst. "Disaster Planning Promises Big Channel Profits." *CRN* 1130 (2005).
18. Sisk, Michael. "Business Continuity: Still Not Entirely Ready For Disaster." *Bank Technology News* 17, no. 12 (2004).
19. The Business Continuity Planning and Disaster Recovery Planning Directory." *Disaster Recovery World*. Available from <http://www.disasterrecoveryworld.com>.
20. Zsidisin, George, A., Gary L. Ragatz and Steven A. Melnyk. "The Dark Side of Supply Chain Management." *Supply Chain Management Review* 9, no. 2 (March 2005).

UNIT 3 DEFINING ORGANIZATION'S BUSINESS CONTINUITY REQUIREMENTS

Structure

- 3.0 Introduction
- 3.1 Objectives
- 3.2 Requirements of Business Continuity
- 3.3 Threats to an Organization
 - 3.3.1 Security Threats to an Organization
 - 3.3.2 Impact of Information Technology Threat
- 3.4 Types of Information Security Controls in Business Continuity
 - 3.4.1 Physical Controls
 - 3.4.2 Technical Controls
 - 3.4.3 Administrative Controls
- 3.5 Optimizing Data Availability for Information hungry Organizations
- 3.6 Planning for Information Resilience
- 3.7 Information Security for the Business Continuity Professional
- 3.8 Disaster and Disaster Recovery in Business Continuity
- 3.9 Risk and Risk Assessment in Business Continuity
- 3.10 Let Us Sum Up
- 3.11 Check Your Progress: The Key
- 3.12 Suggested Readings

3.0 INTRODUCTION

Business continuity is the activity performed by an organization 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.

Business continuity is vital to business success, and in today's interconnected world, virtually every aspect of a company's operation is vulnerable to disruption. Some risks could take your business offline for days, but in a competitive environment, even minutes of downtime could prove fatal. So, how do you determine the resiliency and recovery requirements of your business? How do you identify and integrate critical business and IT priorities into a comprehensive continuity and resiliency program?

Unlike competitors, we leverage industry and IT best practices to better understand your resilience needs, help design a security-rich business continuity plan that addresses your vulnerabilities and compliance requirements, and help you reduce overall risks.

Business Continuity is a management process that identifies potential impacts that threaten an Organization and provides a framework for building resilience with the capability for an effective response to safeguard assets and interests. A successful business works on the basis of revenue growth and loss prevention. Small and medium-sized businesses are particularly hit hard when either one or both of these business requirements suffer. Data leakage, down-time and reputation loss can easily turn away new and existing customers if such situations are not handled appropriately and quickly. This may, in turn, impact on the company's bottom line and ultimately profit margins.

Every organization is aware of the importance of security – security of the building, security for employees and financial security are all a priority; however, an organization comprises many other assets that require security, most notably its IT infrastructure. An organization's network is the lifeline that employees rely on to do their jobs and subsequently make money for the organization. Therefore it's important to recognize that your IT infrastructure is an asset that requires top security.

3.1 OBJECTIVES

After studying this unit, you should be able to:

- understand the requirements of business continuity;
- identify the threats to an organization;
- identify types of information security controls in business continuity;
- discuss information security for the business continuity professional;
- explain information resilience;
- disaster and disaster recovery in business continuity;
- risk and risk assessment in the business continuity.

3.2 REQUIREMENTS OF BUSINESS CONTINUITY

The main requirements of the business continuity for an organization is to maintain business operations under virtually any condition, comply with industry and government regulations and gain the ability to recover from disasters.

Defining Organization's Business Continuity Requirements

- 1) Maintain a continuous flow of your business operations under virtually any condition
- 2) Assess, Design and Plan for a resilient business infrastructure.
- 3) Protect and Recover vital business information.
- 4) Fault tolerant, failure resistant IT infrastructure.³
- 5) Ensure high availability of IT infrastructure
- 6) Identify and integrate critical business and IT priorities into a comprehensive continuity and resiliency program
- 7) Risk assessment and Integrated risk management services ensure secure IT operations and safety of data
- 8) Processes designed keeping in mind dynamic business requirements.

With business becoming more complex and interconnected, the risk and cost of disruption extends well beyond IT, to every aspect of business processes. A disruption in IT infrastructure can put your business in offline mode for several days, when even a few hours of system downtime can critically harm your organization.

3.3 THREATS TO AN ORGANISATION

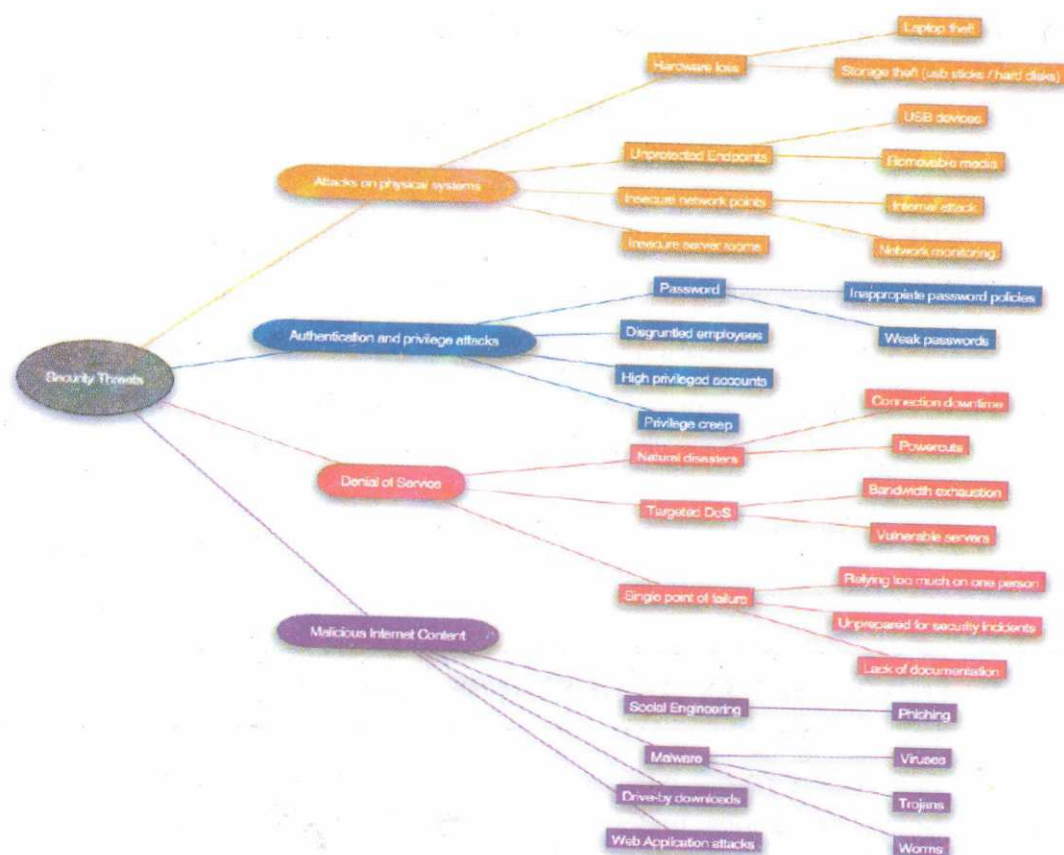


Fig. 1

3.3.1 Security Threats to an Organization

A computer virus outbreak or a network breach can cost a business thousands of dollars. In some cases, it may even lead to legal liability and lawsuits.

The truth is that many organizations would like to have a secure IT environment but very often this need comes into conflict with other priorities. Firms often find the task of keeping the business functions aligned with the security process highly challenging. When economic circumstances look dire, it is easy to turn security into a checklist item that keeps being pushed back. However the reality is that, in such situations, security should be a primary issue. The likelihood of threats affecting your business will probably increase and the impact can be more detrimental if it tarnishes your reputation.

Malicious Internet Content

Most modern small or medium-sized businesses need an Internet connection to operate. If you remove this means of communication, many areas of the organization will not be able to function properly or else they may be forced to revert to old, inefficient systems. Just think how important e-mail has become and that for many organizations this is the primary means of communication. Even phone communications are changing shape with Voice over IP becoming a standard in many organizations.

At some point, most organizations have been the victim of a computer virus attack. While many may have antivirus protection, it is not unusual for an organization of more than 10 employees to use e-mail or the internet without any form of protection. Even large organizations are not spared.

Malware is a term that includes computer viruses, worms, Trojans and any other kinds of malicious software. Employees and end users within an organization may unknowingly introduce malware on the network when they run malicious executable code (EXE files). Sometimes they might receive an e-mail with an attached worm or download spyware when visiting a malicious website. Alternatively, to get work done, employees may decide to install pirated software for which they do not have a license. This software tends to have more code than advertised and is a common method used by malware writers to infect the end user's computers. An organization that operates efficiently usually has established ways to share files and content across the organization. These methods can also be abused by worms to further infect computer systems on the network. Computer malware does not have to be introduced manually or consciously. Basic software packages installed on desktop computers such as Internet Explorer, Firefox, Adobe Acrobat Reader or Flash have their fair share of security vulnerabilities. These security weaknesses are actively exploited by malware writers to automatically infect victim's computers. Such attacks are known as drive-by downloads because the

user does not have knowledge of malicious files being downloaded onto his or her computer.

Social engineering attacks - term refers to a set of techniques whereby attackers make the most of weaknesses in human nature rather than flaws within the technology. A phishing attack is a type of social engineering attack that is normally opportunistic and targets a subset of society. A phishing e-mail message will typically look very familiar to the end users - it will make use of genuine logos and other visuals (from a well-known bank, for example) and will, for all intents and purposes, appear to be the genuine thing. When the end user follows the instructions in the e-mail, he or she is directed to reveal sensitive or private information such as passwords, pin codes and credit card numbers.

Attacks on Physical Systems

Internet-borne attacks are not the only security issue that organizations face. Laptops and mobiles are entrusted with the most sensitive of information about the organization. These devices, whether they are company property or personally owned, often contain company documents and are used to log on to the company network. More often than not, these mobile devices are also used during conferences and travel, thus running the risk of physical theft.

Another threat affecting physical security is that of unprotected endpoints. USB ports and DVD drives can both be used to leak data and introduce malware on the network. A USB stick that is mainly used for work and may contain sensitive documents, becomes a security risk if it is taken home and left lying around and other members of the family use it on their home PC. While the employee may understand the sensitive nature of the information stored on the USB stick, the rest of the family will probably not. They may copy files back and forth without considering the implications. This is typically a case of negligence but it can also be the work of a targeted attack, where internal employees can take large amounts of information out of the company.

Organizations may overlook the importance of securing the physical network and server room to prevent unauthorized persons from gaining access. Open network points and unprotected server rooms can allow disgruntled employees and visitors to connect to the network and launch attacks such as ARP spoofing to capture network traffic with no encryption and steal passwords and content.

Authentication and Privilege Attacks

Passwords remain the number one vulnerability in many systems. It is not an easy task to have a secure system whereby people are required to choose a unique password that others cannot guess but is still easy for them to remember. Nowadays most people have at least five other passwords to

remember, and the password used for company business should not be the same one used for webmail accounts, site memberships and so on.

Password policies can go a long way to mitigate the risk, but if the password policy is too strict people will find ways and means to get around it. They will write the password on sticky notes, share them with their colleagues or simply find a keyboard pattern (1q2w3e4r5t) that is easy to remember but also easy to guess. Most complex password policies can be easily rendered useless by non-technological means.

In Organizations, systems administrators are often found to be doing the work of the network operators and project managers as well as security analysts. Therefore a disgruntled systems administrator will be a major security problem due to the amount of responsibility (and access rights) that he or she holds. With full access privileges, a systems administrator may plan a logic bomb, backdoor accounts or leak sensitive company information that may greatly affect the stability and reputation of the organization.

Additionally, in many cases the systems administrator is the person who sets the passwords for important services or servers. When he or she leaves the organization, these passwords may not be changed (especially if not documented) thus leaving a backdoor for the ex-employee. The company's management team may also have administrative privileges on their personal computers or laptops. The reasons vary but they may want to be able to install new software or simply to have more control of their machines. The problem with this scenario is that one compromised machine is all that an attacker needs to target an organization. The firm itself does not need to be specifically picked out but may simply become a victim of an attack aimed at a particular vulnerable software package.

Even when user accounts on the network are supposed to have reduced privileges, there may be times where privilege creep occurs. For example, a manager that hands over an old project to another manager may retain the old privileges for years even after the handover! When his or her account is compromised, the intruder also gains access to the old project. Employees with mobile devices and laptop computers can pose a significant risk when they make use of unsecured wireless networks whilst attending a conference or during their stay at a hotel. In many cases, inadequate or no encryption is used and anyone 'in between' can view and modify the network traffic. This can be the start of an intrusion leading to compromised company accounts and networks.

Denial of Services

In an attempt to minimize costs, or simply through negligence, most organizations have various single points of failures. Denial of service is an attack that prevents legitimate users from making use of a service and it can be

very hard to prevent. The means to carry out a DoS attack and the motives may vary, but it typically leads to downtime and legitimate customers losing confidence in the organization - and it is not necessarily due to an Internet-borne incident. In 2008 many organizations in the Mediterranean Sea basin and in the Middle East suffered Internet downtime due to damages to the underwater Internet cables. Some of these organizations relied on a single Internet connection, and their business was driven by Internet communications. Having such a single point of failure proved to be very damaging for these organizations in terms of lost productivity and lost business.

Reliability is a major concern for most businesses and their inability to address even one single point of failure can be costly. If an organization is not prepared for a security incident, it will probably not handle the situation appropriately.

3.3.2 Impact of Information Technology Threat

The results of failing to secure your organization's Information Technology network can be far-reaching. Even more devastating than data loss in the event of an IT security breach is the loss of public confidence that may result. The perception of wrongdoing and/or actual fraud can be devastating to your organization and is usually much more difficult to overcome than is the need for simple data recovery. The following categories outline three major impacts of IT threat on your organization

Loss of Integrity

System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an IT system.

Loss of Availability

If a mission-critical IT system is unavailable to its end users, the organization's mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users' performance of their functions in supporting the organization's mission

Loss of Confidentiality

System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the

disclosure of Privacy Act data. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.

Check Your Progress 1

- **Note:** a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) What do you mean by threats in business continuity?

.....

.....

.....

.....

2) Explain different types of threats to an organization.

.....

.....

.....

.....

3) What are the authentication and privilege attacks?

.....

.....

.....

.....

4) Which are the different requirements of Business Continuity?

.....

.....

.....

.....

3.4 TYPES OF INFORMATION SECURITY CONTROLS IN BUSINESS CONTINUITY

Security is generally defined as the freedom from danger or as the condition of safety. Computer security, specifically, is the protection of data in a system against unauthorized disclosure, modification, or destruction and protection of the computer system itself against unauthorized use, modification, or denial of

service. Because certain computer security controls inhibit productivity, security is typically a compromise toward which security practitioners, system users, and system operations and administrative personnel work to achieve a satisfactory balance between security and productivity.

Controls for providing information security can be physical, technical, or administrative. These three categories of controls can be further classified as either **preventive or detective**.

Preventive controls attempt to avoid the occurrence of unwanted events, whereas detective controls attempt to identify unwanted events after they have occurred. Preventive controls inhibit the free use of computing resources and therefore can be applied only to the degree that the users are willing to accept. Effective security awareness programs can help increase users' level of tolerance for preventive controls by helping them understand how such controls enable them to trust their computing systems. Common detective controls include audit trails, intrusion detection methods, and checksums.

Three other types of controls supplement preventive and detective controls. They are usually described as **deterrent, corrective, and recovery**.

Deterrent controls are intended to discourage individuals from intentionally violating information security policies or procedures. These usually take the form of constraints that make it difficult or undesirable to perform unauthorized activities or threats of consequences that influence a potential intruder to not violate security (e.g., threats ranging from embarrassment to severe punishment).

Corrective controls either remedy the circumstances that allowed the unauthorized activity or return conditions to what they were before the violation. Execution of corrective controls could result in changes to existing physical, technical, and administrative controls.

Recovery controls restore lost computing resources or capabilities and help the organization recover monetary losses caused by a security violation.

Deterrent, corrective, and recovery controls are considered to be special cases within the major categories of physical, technical, and administrative controls; they do not clearly belong in either preventive or detective categories. For example, it could be argued that deterrence is a form of prevention because it can cause an intruder to turn away; however, deterrence also involves detecting violations, which may be what the intruder fears most. Corrective controls, on the other hand, are not preventive or detective, but they are clearly linked with technical controls when antiviral software eradicates a virus or with administrative controls when backup procedures enable restoring a damaged data base. Finally, recovery controls are neither preventive nor detective but are included in administrative controls as disaster recovery or contingency plans.

3.4.1 Physical Controls

Physical security is the use of locks, security guards, badges, alarms, and similar measures to control access to computers, related equipment (including utilities), and the processing facility itself. In addition, measures are required for protecting computers, related equipment, and their contents from espionage, theft, and destruction or damage by accident, fire, or natural disaster (e.g., floods and earthquakes).

Preventive Physical Controls

Preventive physical controls are employed to prevent unauthorized personnel from entering computing facilities (i.e., locations housing computing resources, supporting utilities, computer hard copy, and input data media) and to help protect against natural disasters. Examples of these controls include:

Backup Files and Documentation

Should an accident or intruder destroy active data files or documentation, it is essential that backup copies be readily available. Backup files should be stored far enough away from the active data or documentation to avoid destruction by the same incident that destroyed the original. Backup material should be stored in a secure location constructed of noncombustible materials, including two-hour-rated fire walls. Backups of sensitive information should have the same level of protection as the active files of this information; it is senseless to provide tight security for data on the system but lax security for the same data in a backup location.

Fences

Although fences around the perimeter of the building do not provide much protection against a determined intruder, they do establish a formal no trespassing line and can dissuade the simply curious person. Fences should have alarms or should be under continuous surveillance by guards, dogs, or TV monitors.

Security Guards

Security guards are often stationed at the entrances of facilities to intercept intruders and ensure that only authorized persons are allowed to enter. Guards are effective in inspecting packages or other hand-carried items to ensure that only authorized, properly described articles are taken into or out of the facility. The effectiveness of stationary guards can be greatly enhanced if the building is wired with appropriate electronic detectors with alarms or other warning indicators terminating at the guard station. In addition, guards are often used to patrol unattended spaces inside buildings after normal working hours to deter intruders from obtaining or profiting from unauthorized access.

Badge Systems

Physical access to computing areas can be effectively controlled using a badge system. With this method of control, employees and visitors must wear appropriate badges whenever they are in access-controlled areas. Badge-reading systems programmed to allow entrance only to authorized persons can then easily identify intruders.

Double Door Systems

Double door systems can be used at entrances to restricted areas (e.g., computing facilities) to force people to identify themselves to the guard before they can be released into the secured area. Double doors are an excellent way to prevent intruders from following closely behind authorized persons and slipping into restricted areas.

Locks and Keys

Locks and keys are commonly used for controlling access to restricted areas. Because it is difficult to control copying of keys, many installations use cipher locks (i.e., combination locks containing buttons that open the lock when pushed in the proper sequence). With cipher locks, care must be taken to conceal which buttons are being pushed to avoid a compromise of the combination.

Backup Power

Backup power is necessary to ensure that computer services are in a constant state of readiness and to help avoid damage to equipment if normal power is lost. For short periods of power loss, backup power is usually provided by batteries. In areas susceptible to outages of more than 15–30 min., diesel generators are usually recommended.

Biometric Access Controls

Biometric identification is a more sophisticated method of controlling access to computing facilities than badge readers, but the two methods operate in much the same way. Biometrics used for identification include fingerprints, handprints, voice patterns, signature samples, and retinal scans. Because biometrics cannot be lost, stolen, or shared, they provide a higher level of security than badges. Biometric identification is recommended for high-security, low-traffic entrance control.

Site Selection

The site for the building that houses the computing facilities should be carefully chosen to avoid obvious risks. For example, wooded areas can pose a fire hazard, areas on or adjacent to an earthquake fault can be dangerous and

sites located in a flood plain are susceptible to water damage. In addition, locations under an aircraft approach or departure route are risky, and locations adjacent to railroad tracks can be susceptible to vibrations that can precipitate equipment problems.

Fire Extinguishers

The control of fire is important to prevent an emergency from turning into a disaster that seriously interrupts data processing. Computing facilities should be located far from potential fire sources (e.g., kitchens or cafeterias) and should be constructed of noncombustible materials. Furnishings should also be noncombustible. It is important that appropriate types of fire extinguishers be conveniently located for easy access. Employees must be trained in the proper use of fire extinguishers and in the procedures to follow should a fire break out.

Automatic sprinklers are essential in computer rooms and surrounding spaces and when expensive equipment is located on raised floors. Sprinklers are usually specified by insurance companies for the protection of any computer room that contains combustible materials. However, the risk of water damage to computing equipment is often greater than the risk of fire damage. Therefore, carbon dioxide extinguishing systems were developed; these systems flood an area threatened by fire with carbon dioxide, which suppresses fire by removing oxygen from the air. Although carbon dioxide does not cause water damage, it is potentially lethal to people in the area and is now used only in unattended areas.

Current extinguishing systems flood the area with Halon, which is usually harmless to equipment and less dangerous to personnel than carbon dioxide. At a concentration of about 10%, Halon extinguishes fire and can be safely breathed by humans. However, higher concentrations can eventually be a health hazard. In addition, the blast from releasing Halon under pressure can blow loose objects around and can be a danger to equipment and personnel. For these reasons and because of the high cost of Halon, it is typically used only under raised floors in computer rooms. Because it contains chlorofluorocarbons, it will soon be phased out in favor of a gas that is less hazardous to the environment.

Detective Physical Controls

Detective physical controls warn protective services personnel that physical security measures are being violated. Examples of these controls include:

Motion Detectors

In computing facilities that usually do not have people in them, motion detectors are useful for calling attention to potential intrusions. Motion detectors must be constantly monitored by guards.

Fire and Smoke Detectors

Fire and smoke detectors should be strategically located to provide early warning of a fire. All fire detection equipment should be tested periodically to ensure that it is in working condition.

Closed-Circuit Television Monitors

Closed-circuit televisions can be used to monitor the activities in computing areas where users or operators are frequently absent. This method helps detect individuals behaving suspiciously.

Sensors and Alarms

Sensors and alarms monitor the environment surrounding the equipment to ensure that air and cooling water temperatures remain within the levels specified by equipment design. If proper conditions are not maintained, the alarms summon operations and maintenance personnel to correct the situation before a business interruption occurs..

3.4.2 Technical Controls

Technical security involves the use of safeguards incorporated in computer hardware, operations or applications software, communications hardware and software, and related devices. Technical controls are sometimes referred to as logical controls.

Preventive Technical Controls

Preventive technical controls are used to prevent unauthorized personnel or programs from gaining remote access to computing resources. Examples of these controls include:

Access Control Software

The purpose of access control software is to control sharing of data and programs between users. In many computer systems, access to data and programs is implemented by access control lists that designate which users are allowed access. Access control software provides the ability to control access to the system by establishing that only registered users with an authorized log-on ID and password can gain access to the computer system.

After access to the system has been granted, the next step is to control access to the data and programs residing in the system. The data or program owner can establish rules that designate who is authorized to use the data or program.

Antivirus Software

Viruses have reached epidemic proportions throughout the micro computing world and can cause processing disruptions and loss of data as well as

significant loss of productivity while cleanup is conducted. In addition, new viruses are emerging at an ever-increasing rate — currently about one every 48 hours. It is recommended that antivirus software be installed on all microcomputers to detect, identify, isolate, and eradicate viruses. This software must be updated frequently to help fight new viruses. In addition, to help ensure that viruses are intercepted as early as possible, antivirus software should be kept active on a system, not used intermittently at the discretion of users.

Library Control Systems

These systems require that all changes to production programs be implemented by library control personnel instead of the programmers who created the changes. This practice ensures separation of duties, which helps prevent unauthorized changes to production programs.

Passwords

Passwords are used to verify that the user of an ID is the owner of the ID. The ID-password combination is unique to each user and therefore provides a means of holding users accountable for their activity on the system.

Fixed passwords that are used for a defined period of time are often easy for hackers to compromise; therefore, great care must be exercised to ensure that these passwords do not appear in any dictionary. Fixed passwords are often used to control access to specific data bases. In this use, however, all persons who have authorized access to the data base use the same password; therefore, no accountability can be achieved.

Currently, dynamic or one-time passwords, which are different for each log-on, are preferred over fixed passwords. Dynamic passwords are created by a token that is programmed to generate passwords randomly.

Smart Cards

Smart cards are usually about the size of a credit card and contain a chip with logic functions and information that can be read at a remote terminal to identify a specific user's privileges. Smart cards now carry prerecorded, usually encrypted access control information that is compared with data that the user provides (e.g., a personal ID number or biometric data) to verify authorization to access the computer or network.

Encryption

Encryption is defined as the transformation of plaintext (i.e., readable data) into ciphertext (i.e., unreadable data) by cryptographic techniques. Encryption is currently considered to be the only sure way of protecting data from disclosure during network transmissions.

Encryption can be implemented with either hardware or software. Software-based encryption is the least expensive method and is suitable for applications involving low-volume transmissions; the use of software for large volumes of data results in an unacceptable increase in processing costs. Because there is no overhead associated with hardware encryption, this method is preferred when large volumes of data are involved.

Dial-Up Access Control and Callback Systems

Dial-up access to a computer system increases the risk of intrusion by hackers. In networks that contain personal computers or are connected to other networks, it is difficult to determine whether dial-up access is available or not because of the ease with which a modem can be added to a personal computer to turn it into a dial-up access point. Known dial-up access points should be controlled so that only authorized dial-up users can get through.

Currently, the best dial-up access controls use a microcomputer to intercept calls, verify the identity of the caller (using a dynamic password mechanism), and switch the user to authorized computing resources as requested. Previously, call-back systems intercepted dial-up callers, verified their authorization and called them back at their registered number, which at first proved effective; however, sophisticated hackers have learned how to defeat this control using call-forwarding techniques.

Detective Technical Controls

Detective technical controls warn personnel of violations or attempted violations of preventive technical controls. Examples of these include audit trails and intrusion detection expert systems, which are discussed in the following sections.

Audit Trails

An audit trail is a record of system activities that enables the reconstruction and examination of the sequence of events of a transaction, from its inception to output of final results. Violation reports present significant, security-oriented events that may indicate either actual or attempted policy transgressions reflected in the audit trail. Violation reports should be frequently and regularly reviewed by security officers and data base owners to identify and investigate successful or unsuccessful unauthorized accesses.

Intrusion Detection Systems

These expert systems track users (on the basis of their personal profiles) while they are using the system to determine whether their current activities are consistent with an established norm. If not, the user's session can be terminated or a security officer can be called to investigate. Intrusion detection can be

especially effective in cases in which intruders are pretending to be authorized users or when authorized users are involved in unauthorized activities.

3.4.3 Administrative Controls

Administrative, or personnel, security consists of management constraints, operational procedures, accountability procedures, and supplemental administrative controls established to provide an acceptable level of protection for computing resources. In addition, administrative controls include procedures established to ensure that all personnel who have access to computing resources have the required authorizations and appropriate security clearances.

Preventive Administrative Controls

Preventive administrative controls are personnel-oriented techniques for controlling people's behavior to ensure the confidentiality, integrity, and availability of computing data and programs. Examples of preventive administrative controls include:

Security Awareness and Technical Training

Security awareness training is a preventive measure that helps users to understand the benefits of security practices. If employees do not understand the need for the controls being imposed, they may eventually circumvent them and thereby weaken the security program or render it ineffective.

Technical training can help users prevent the most common security problem — errors and omissions — as well as ensure that they understand how to make appropriate backup files and detect and control viruses. Technical training in the form of emergency and fire drills for operations personnel can ensure that proper action will be taken to prevent such events from escalating into disasters.

Separation of Duties

This administrative control separates a process into component parts, with different users responsible for different parts of the process. Judicious separation of duties prevents one individual from obtaining control of an entire process and forces collusion with others in order to manipulate the process for personal gain.

Recruitment and Termination Procedures

Appropriate recruitment procedures can prevent the hiring of people who are likely to violate security policies. A thorough background investigation should be conducted, including checking on the applicant's criminal history and

references. Although this does not necessarily screen individuals for honesty and integrity, it can help identify areas that should be investigated further.

Three types of references should be obtained: (1) employment, (2) character, and (3) credit. Employment references can help estimate an individual's competence to perform, or be trained to perform, the tasks required on the job. Character references can help determine such qualities as trustworthiness, reliability, and ability to get along with others. Credit references can indicate a person's financial habits, which in turn can be an indication of maturity and willingness to assume responsibility for one's own actions.

In addition, certain procedures should be followed when any employee leaves the company, regardless of the conditions of termination. Any employee being involuntarily terminated should be asked to leave the premises immediately upon notification, to prevent further access to computing resources. Voluntary terminations may be handled differently, depending on the judgment of the employee's supervisors, to enable the employee to complete work in process or train a replacement.

All authorizations that have been granted to an employee should be revoked upon departure. If the departing employee has the authority to grant authorizations to others, these other authorizations should also be reviewed. All keys, badges, and other devices used to gain access to premises, information, or equipment should be retrieved from the departing employee. The combinations of all locks known to a departing employee should be changed immediately. In addition, the employee's log-on IDs and passwords should be canceled, and the related active and backup files should be either deleted or reassigned to a replacement employee.

Any special conditions to the termination (e.g., denial of the right to use certain information) should be reviewed with the departing employee; in addition, a document stating these conditions should be signed by the employee. All terminations should be routed through the computer security representative for the facility where the terminated employee works to ensure that all information system access authority has been revoked.

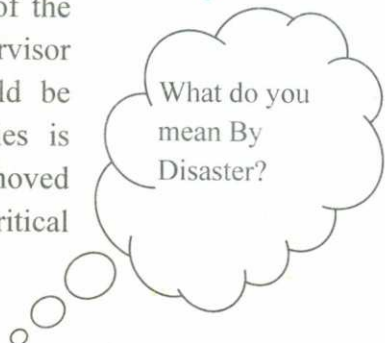
Security Policies and Procedures

Appropriate policies and procedures are key to the establishment of an effective information security program. Policies and procedures should reflect the general policies of the organization as regards the protection of information and computing resources. Policies should cover the use of computing resources, marking of sensitive information, movement of computing resources outside the facility, introduction of personal computing equipment and media into the facility, disposal of sensitive waste, and computer and data security incident reporting. Enforcement of these policies is essential to their effectiveness.

Supervision

Often, an alert supervisor is the first person to notice a change in an employee's attitude. Early signs of job dissatisfaction or personal distress should prompt supervisors to consider subtly moving the employee out of a critical or sensitive position.

Supervisors must be thoroughly familiar with the policies and procedures related to the responsibilities of their department. Supervisors should require that their staff members comply with pertinent policies and procedures and should observe the effectiveness of these guidelines. If the objectives of the policies and procedures can be accomplished more effectively, the supervisor should recommend appropriate improvements. Job assignments should be reviewed regularly to ensure that an appropriate separation of duties is maintained, that employees in sensitive positions are occasionally removed from a complete processing cycle without prior announcement, and that critical or sensitive jobs are rotated periodically among qualified personnel.



What do you
mean By
Disaster?

Disaster Recovery, Contingency, and Emergency Plans

The disaster recovery plan is a document containing procedures for emergency response, extended backup operations, and recovery should a computer installation experience a partial or total loss of computing resources or physical facilities (or of access to such facilities). The primary objective of this plan, used in conjunction with the contingency plans, is to provide reasonable assurance that a computing installation can recover from disasters, continue to process critical applications in a degraded mode, and return to a normal mode of operation within a reasonable time. A key part of disaster recovery planning is to provide for processing at an alternative site during the time that the original facility is unavailable.

Contingency and emergency plans establish recovery procedures that address specific threats. These plans help prevent minor incidents from escalating into disasters. For example, a contingency plan might provide a set of procedures that defines the condition and response required to return a computing capability to nominal operation; an emergency plan might be a specific procedure for shutting down equipment in the event of a fire or for evacuating a facility in the event of an earthquake.

User Registration for Computer Access

Formal user registration ensures that all users are properly authorized for system and service access. In addition, it provides the opportunity to acquaint users with their responsibilities for the security of computing resources and to obtain their agreement to comply with related policies and procedures.

Detective Administrative Controls

Detective administrative controls are used to determine how well security policies and procedures are complied with, to detect fraud, and to avoid employing persons that represent an unacceptable security risk. This type of control includes:

Security Reviews and Audits

Reviews and audits can identify instances in which policies and procedures are not being followed satisfactorily. Management involvement in correcting deficiencies can be a significant factor in obtaining user support for the computer security program.

Performance Evaluations

Regularly conducted performance evaluations are an important element in encouraging quality performance. In addition, they can be an effective forum for reinforcing management's support of information security principles.

Required Vacations

Tense employees are more likely to have accidents or make errors and omissions while performing their duties. Vacations contribute to the health of employees by relieving the tensions and anxieties that typically develop from long periods of work. In addition, if all employees in critical or sensitive positions are forced to take vacations, there will be less opportunity for an employee to set up a fraudulent scheme that depends on the employee's presence (e.g., to maintain the fraud's continuity or secrecy). Even if the employee's presence is not necessary to the scheme, required vacations can be a deterrent to embezzlement because the employee may fear discovery during his or her absence.

Background Investigations

Background investigations may disclose past performances that might indicate the potential risks of future performance. Background investigations should be conducted on all employees being considered for promotion or transfer into a position of trust; such investigations should be completed before the employee is actually placed in a sensitive position. Job applicants being considered for sensitive positions should also be investigated for potential problems. Companies involved in government-classified projects should conduct these investigations while obtaining the required security clearance for the employee.

Rotation of Duties

Like required vacations, rotation of duties (i.e., moving employees from one job to another at random intervals) helps deter fraud. An additional benefit is

that as a result of rotating duties, employees are cross-trained to perform each other's functions in case of illness, vacation, or termination.

Check Your Progress 2

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) What do you mean by security?

.....

.....

.....

.....

2) How Information Security is controlled in Business Continuity of an organization.

.....

.....

.....

.....

3) What are the protective and detective types of security controls?

.....

.....

.....

.....

4) List the different type of security controls.

.....

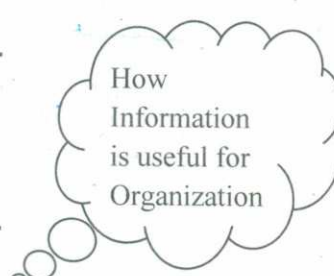
.....

.....

.....

3.5 OPTIMIZING DATA AVAILABILITY FOR THE INFORMATION HUNGRY ORGANISATIONS

Information is the fuel for click-driven commerce as well as bricks and mortar businesses. How you use information is a critical way to differentiate the organization from every other competitor. Organizations that use information in new, vital ways can now reach more informed decisions faster. This accelerating pace of decision-making can surely deliver an advantage. Small



How
Information
is useful for
Organization

and mid-sized businesses, looking for every opportunity to compete, will surely benefit the most.

The demands on a business today – increased global competition, lower barriers to entry, lower profit margins – are creating an ever-increasing need for access to data. In this environment the accelerating “time-to action” will become the new business precept. At its core is the ability for every organization to ensure that the right information reaches the right people at the right time. The challenge: dealing with the every increasing volume of data and turning it into something meaningful.

Organizations that are the most successful at collecting, evaluating and applying information are consistently industry leaders.

Business Resilience will provide some insights into how to solve these challenges and help organizations find new ways to deliver the right information at accelerated speeds throughout the business. After all, users won't wait. And customers won't wait. The business will look to IT to speed up the time-to-decision.

3.6 PLANNING FOR INFORMATION RESILIENCE

Understanding the Power of Information Availability to Deliver Value for the Organization

Over the last few years, every business has faced an onslaught of challenges: global economic volatility, fierce competition, customer churn, mergers and acquisitions, rising security concerns and waves of regulatory compliance issues. Meanwhile, stakeholders continue to demand that top executives increase profits, lower costs, expand market share and grow revenue.

To solve these issues, much has been demanded from your information technology infrastructure. You depend on IT to keep the business running, to harness complex, often competing, initiatives into a larger, strategic vision that supports the business. Most importantly, you need the resilient information and applications, systems and security that can support the business wherever the future leads it.

How Does Information Availability Enable Business Resilience?

Information resilience encompasses most of the data, applications and systems aspects of what we know as business continuity, continuous availability, high availability, and data protection and recovery. Information resilience looks at the long-term viability of the IT “dial tone” that runs your business today, tomorrow and long into the future.

Because a business thrives on information, the availability of that information plays a key role in business resilience. Any interruption or interference (downtime) that makes your information or applications inaccessible or inaccurate adds delay to your go-to-market processes, supply chain, analyses and every day, even vital, decisions.

Downtime prevents immediate action from your customers, employees and business partners. Many business executives are not even aware of this built-in hidden, but altogether unnecessary cost. A truly resilient business, however, will take steps to solve downtime issues throughout all of its business processes and in its IT infrastructure.

Downtime: Bad for the Bottom Line

Even the most highly effective information-driven organization inevitably suffers some form of downtime or interference to access and information flow. But the most resilient organizations have taken steps to severely reduce its impact and costs.

Causes of Downtime: Unplanned and Planned Interruptions

While some unplanned downtime results from weather or other disaster, most happens because of hardware or application failures, human errors and security violations. Surprisingly though, studies show that planned interruptions (downtime) caused by routine daily/weekly backups, system upgrades, performance tuning and batch jobs create 70-90 percent of interruptions for most businesses.

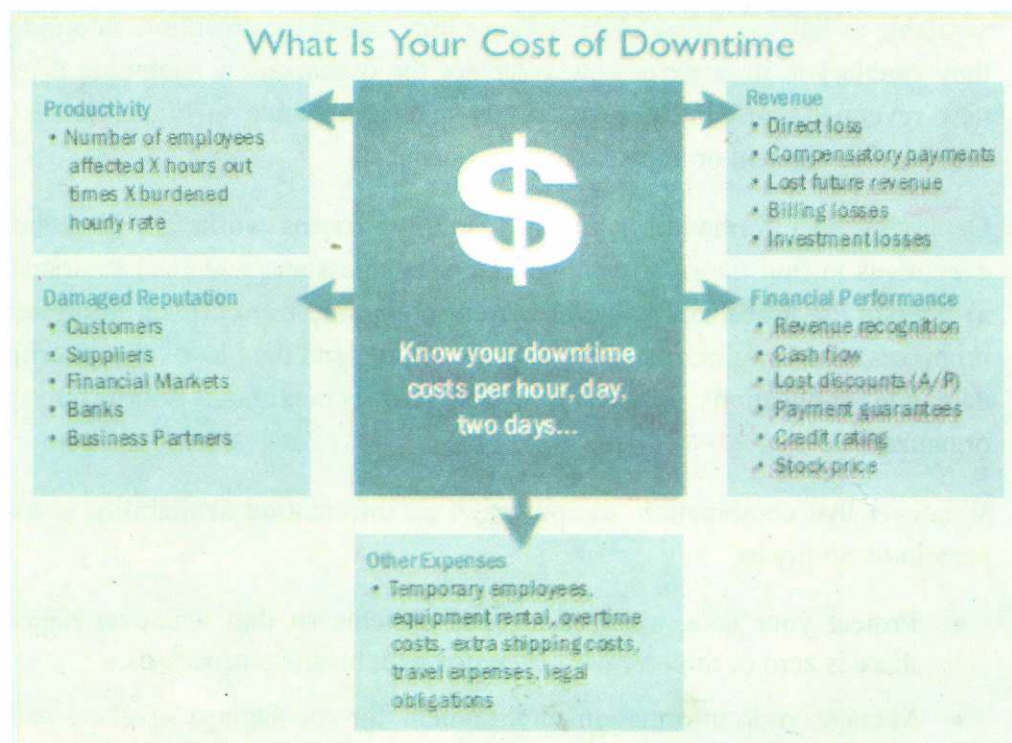
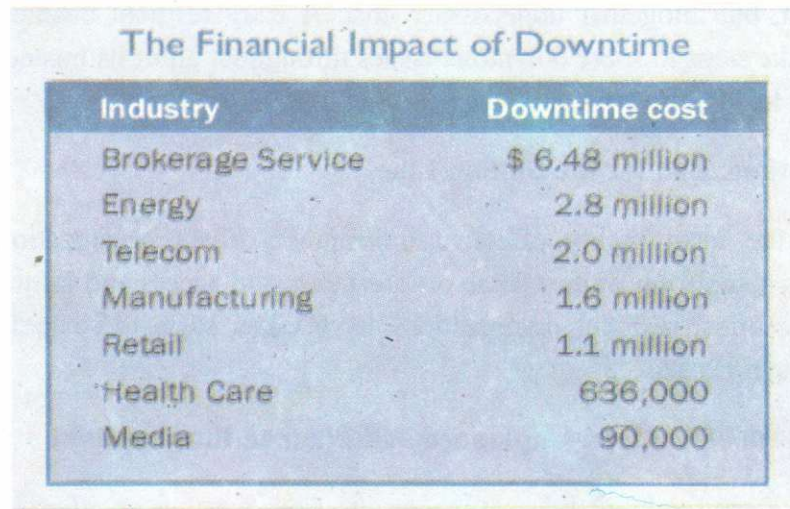


Fig. 2

Whatever its cause, downtime adds no value to your business goals. It's the equivalent of turning out the lights and sending everyone home. This downtime interferes with and delays the forward movement of your strategies and reduces the profitability and return your shareholders expect. For example, a study by a major business continuity group showed that 54 percent of surveyed businesses indicated that an hour of downtime would cost between \$51,000 – \$1 million (US). Of even more concern, a similar survey found that on average restoring access and availability to critical information systems would take 9–12 hours.



Industry	Downtime cost
Brokerage Service	\$ 6.48 million
Energy	2.8 million
Telecom	2.0 million
Manufacturing	1.6 million
Retail	1.1 million
Health Care	636,000
Media	90,000

Fig. 3

Turning Downtime to Value-Producing Uptime: Enhancing Business Resilience

Information availability software solutions help drive business resilience because they ensure that information and applications remain as accessible and available as needed. In addition, because they transform downtime into uptime they enable you to uncover new value for the organization, including driving new revenue, profitability, productivity and compliance to higher levels no matter what planned or unplanned events occur.

Deploying an information availability solution means working with your IT executives to find the right combination of business and technical solutions to a) liberate the unrealized value of current downtime from critical information processes; and b) minimize acceptable downtime and data loss for non-critical data and applications so they can deliver the maximum return for your organization.

Whatever that combination, the power of an information availability solution rests in its ability to:

- Protect your data, applications and systems so that whatever happens there is zero or minimum interference with business processes.
- Manage your information environment for the highest level of value-producing uptime with extensive automation to minimize impact on staff, IT resources or new skill requirements.

- Assure the integrity and quality of your environment for maximum confidence in the ability of the business to continue without interruption or with as minimal impact as possible.

How to Establish Information Resiliency Objectives

When it comes to information resilience, you will want to focus on the most critical applications and business processes.

For example, you will want to establish objectives for recovering from a business outage—whether a planned or unplanned. The recovery time objective (RTO) is the targeted amount of time required to resume and recover application functionality. This is essentially the amount of time that you can afford to be offline. The recovery point objective (RPO) defines how much data you can afford to lose or how far back in time you can afford to go when you resume your application functionality.

Obviously, every company would like to have RTO and RPO as close as possible to zero but availability solutions with lower RTOs and RPOs generally are more expensive to purchase and operate. So it becomes important to determine the economically appropriate level for different applications.

3.7 INFORMATION SECURITY FOR THE BUSINESS CONTINUITY PROFESSIONAL

Traditionally, the focus of Information Security efforts has centered on virus detection and prevention, hacking into systems and securing networks from unintended intrusions.

While these are still admirable areas to work on and provide measurable goals for internal reporting, they are just the tip of the iceberg. The weakest links in our information security protocols are employees.

People are a critical factor in ensuring the security of computer systems and information resources. Information security needs to begin on the desk PC or the laptop that travels between work and home. The role of the business continuity professional is to be aware of threats, make all employees aware of threats, and to work with the information security professionals to ensure that policies and procedures are in place to protect the organization.

System Security Plan

Every organization should have a system security plan as part of their overall business continuity, disaster recovery and resilience program. The plan delineates responsibilities and expected behavior of all individuals who access the system. The plan should include a comprehensive IT Information Security policy that adequately addresses all major areas of IT operations. At a

minimum the policy should address the terms and conditions covering the use of the network, network etiquette, sanctions for noncompliance, and passwords.

Policies should prohibit use of office computers for personal purposes unrelated to the operation of the organization. The policy should be followed up with regular inspections to monitor computer and laptop usage.

Personnel Security

Many important issues in computer security involve human users, designers, implementers, and managers. A broad range of security issues relates to how individuals interact with computers, and the access and authorities needed to do their jobs.

It is important to include the following policies and procedures when evaluating personnel security:

- Personnel screening
- Personnel termination
- Personnel transfer
- Access agreements
- Third-party personnel security
- Personnel sanctions

IT policies should include procedures for acceptable computer, internet and e-mail use, data and virus protection, password security, remote access and internet privacy.

PC or Laptop Security

A key area where many organizations struggle is on the corporate laptop issue. A huge potential benefit to the BC program is providing laptops to key personnel that are taken home each and every evening. This positions BCP team members and key staff with the ability to work remotely if their primary work area is not available.

However, the data on laptops needs to be kept safe, backed up and synchronized. While the mean time between failures is significantly longer than in the past, this can give the end user a false sense of security. The reality is the data can be compromised by viruses, hacking, hardware failure or environmental issues. Laptops can also be lost or stolen, and the plan should reflect these risks. Laptops are cheap, data are not.

Account Access as Part of Information Security

Organizations should have some type of account naming scheme. When a new end user is identified, he should be issued an account based on company

policies. This would include access to the network, mail systems, data bases, applications and information sources. Each of the access rights granted should be on a need to use basis.

Account access for production systems should only have accounts that are directly traceable back to an owner. There is a need for system accounts, batch or other processing accounts, but they need to have an owner that is responsible for that account. As an application migrates from development to test and then to production, all the earlier accounts and capabilities should be deleted and only those required accounts reset into the system with proper authorizations.

The following combinations of functions should not be performed by the same individual:

- Data entry and verification of data
- Data entry and its reconciliation of output
- Input of transactions for incompatible processing functions
- Data entry and supervisory authorization functions

Check Your Progress 3

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) What is Information resilience?

.....

.....

.....

.....

2) How Does Information Availability Enable Business Resilience?

.....

.....

.....

.....

3) What do you mean by Information security for the business continuity professional?

.....

.....

.....

.....

4) What are the causes of downtime in Business Continuity?

3.8 DISASTER AND DISASTER RECOVERY IN BUSINESS CONTINUITY

Disaster recovery is the process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster. Disaster recovery is a subset of business continuity. While business continuity involves planning for keeping all aspects of a business functioning in the midst of disruptive events, disaster recovery focuses on the IT or technology systems that support business functions.

Classification of Disasters

Disasters can be classified in two broad categories. The first is natural disasters such as floods, hurricanes, tornadoes or earthquakes. While preventing a natural disaster is very difficult, measures such as good planning which includes mitigation measures can help reduce or avoid losses. The second category is man made disasters. These include hazardous material spills, infrastructure failure, or bio-terrorism. In these instances surveillance and mitigation planning are invaluable towards avoiding or lessening losses from these events.

The Need for Business Continuity/Disaster Recovery Planning and Management

In the aftermath of recent natural disasters, terrorism, and equipment breakdown, businesses have recognized more than ever the need for an organization to be prepared. Companies are striving to meet the demand for continuous service. With the growth of e-commerce and other factors driving system availability expectations toward 24x365, the average organization's requirement for recovery time from a major system outage now ranges between two and 24 hours. This requirement is pushed by the expectation an organization faces on all sides:

- Customers expect supplies and services to continue— or resume rapidly— in all situations.
- Shareholders expect management control to remain operational through any crisis.

- Employees expect both their lives and livelihoods to be protected.
- Suppliers expect their revenue streams to continue.
- Regulatory agencies expect their requirements to be met, regardless of circumstances.
- Insurance companies expect due care to be exercised.

Business Survival in an Uncertain World

Business survival necessitates planning for every type of business disruption including— but by no means limited to— the categories of natural disasters; hardware and communications failures; internal or external sabotage or acts of terrorism; and the failures of supply chain and sales affiliate organizations. While such disruptions cannot be predicted, they can wreak havoc upon the business, with results ranging from insured losses of replaceable tangibles to uninsurable capital losses to customer dissatisfaction and possible desertion to complete insolvency. Other business disruptions, such as a hurricane, may give advance warning. Others, such as terrorism, flash floods, fire, etc., can strike without notice.

A business continuity strategy, then, is a high-value— but high-maintenance— proposition. Business continuity embraces a broad spectrum of technologies: old and new, paper-based and electronic, manual and automated, individual and integrated.

The key challenge of business continuity preparation is not technology, however, but the internal marketing “business” aspects that begin at the foundation level of any project and continue throughout its life cycle: justification, executive buy-in, broad organizational support, and governance and politics. Perhaps the most important point to make about business continuity support technologies is that their effectiveness depends entirely upon the organization’s top-down commitment to the entire project, including the updating and testing necessary for maintenance.

Strategies for Disaster Recovery

Prior to selecting a disaster recovery strategy, a disaster recovery planner should refer to their organization's business continuity plan which should indicate the key metrics of recovery point objective (RPO) and recovery time objectives (RTO) for various business processes (such as the process to run payroll, generate an order, etc.). The metrics specified for the business processes must then be mapped to the underlying IT systems and infrastructure that support those processes.

- **Recovery point objective (RPO)** describes the acceptable amount of data loss measured in time.

The recovery point objective is the point in time to which you must recover data as defined by your organization. This is generally a definition of what an organization determines is an "acceptable loss" in a disaster situation. The RPO allows an organization to define a window of time before a disaster during which data may be lost. The value of the data in this window can then be weighed against the cost of the additional disaster prevention or loss-prevention measures that would be necessary to close the window.

RPO is independent of the time it takes to get a non-functional system back on-line (the recovery time objective). If the RPO of a company is two hours, then when a system is brought back on-line after a disaster, all data must be restored to a point within two hours before the disaster. But the company has acknowledged that data in the two hours immediately preceding the disaster may be lost (the acceptable loss window is two hours).

- **The recovery time objective (RTO)** is the duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.

It includes the time for trying to fix the problem without a recovery, the recovery itself, tests and the communication to the users. Decision time for users representative is not included.

The business continuity timeline usually runs parallel with an incident management timeline and may start at the same, or different, points.

In accepted business continuity planning methodology the RTO is established during the Business Impact Analysis (BIA) by the owner of a process (usually in conjunction with the business continuity planner). The RTOs are then presented to senior management for acceptance.

The RTO attaches to the business process and not the resources required to support the process.

The RTO and the results of the BIA in its entirety provide the basis for identifying and analyzing viable strategies for inclusion in the business continuity plan. Viable strategy options would include any which would enable resumption of a business process in a time frame at or near the RTO. This would include alternate or manual workaround procedures and would not necessarily require computer systems to meet the RTOs

The "O" in RTO stands for objective, not mandate. In reality, tactics are often selected that will not meet the RTO. In this instance the RTO will not be met but should still remain an objective of future strategy revision.

Once the RTO and RPO metrics have been mapped to IT infrastructure, the DR planner can determine the most suitable recovery strategy for each system. An

important note here however is that the business ultimately sets the IT budget and therefore the RTO and RPO metrics need to fit with the available budget. While most business unit heads would like zero data loss and zero time loss, the cost associated with that level of protection may make the desired high availability solutions impractical.

The following is a list of the most common strategies for data protection.

- Backups made to tape and sent off-site at regular intervals
- Backups made to disk on-site and automatically copied to off-site disk, or made directly to off-site disk
- Replication of data to an off-site location, which overcomes the need to restore the data (only the systems then need to be restored or synchronized). This generally makes use of storage area network (SAN) technology
- High availability systems which keep both the data and system replicated off-site, enabling continuous access to systems and data

In many cases, an organization may elect to use an outsourced disaster recovery provider to provide a stand-by site and systems rather than using their own remote facilities.

In addition to preparing for the need to recover systems, organizations must also implement precautionary measures with an objective of preventing a disaster in the first place. These may include some of the following:

- Local mirrors of systems and/or data and use of disk protection technology such as RAID
- Surge protectors — to minimize the effect of power surges on delicate electronic equipment
- Uninterruptible power supply (UPS) and/or backup generator to keep systems going in the event of a power failure
- Fire preventions — alarms, fire extinguishers
- Anti-virus software and other security measures

Differences between Disaster Recovery and Business Continuity

There are 13 differences between disaster recovery and business continuity.

1. **Area of Emphasis:** Decades ago companies started relying more and more on computer technology for their critical businesses and core competencies. When computers experienced sustained outages, companies would feel the business impact. The thought of losing all computer services for days at a time due to natural or manmade disasters caused many companies to emphasize the quick recovery of their data centers. Until recently many

people interpreted the term disaster recovery to mean the quick resumption of data center services.

Companies eventually realized that major disasters would not only disrupt computer services, but other critical business processes having little or nothing to do with IT. Emphasis gradually shifted from not recovering the computer services of the data center, but of recovering business processes across the whole enterprise. This shift of emphasis is how IT disaster recovery evolved into enterprise-wide business continuity.

2. **Approach:** The act of recovering from any disaster is, by definition, a reactive response. The approach most IT organizations used to take in regards to disaster recovery was to focus on the recovery steps needed to restore processors, systems, or voice and data network. Reaction time was a key aspect of this process. Business continuity begins with a business impact analysis (BIA) that identifies and prioritizes critical business functions and their dependencies. The BIA also includes an assessment of threats and vulnerabilities to these business functions. Risk managers and business continuity planners can then use this BIA information to mitigate threats and vulnerabilities in a much more proactive manner.

Table 1: Differences between Disaster Recovery and Business Continuity

Category	Disaster Recovery	Business Continuity
1. Area of Emphasis	Data Center	Enterprise
2. Approach	Reactive	Proactive
3. Orientation	Technology	Business
4. Decade of Origin	1970's	1990's
5. Degree of Customer Involvement	Minimal	Extensive
6. Variety of Support Groups	Few	Diverse
7. Number of Users Participating	None	Many
8. Primary Metrics	MTBF/MTTR	RPO/PTO
9. Management Style	Dictatorial	Collaborative
10. Sponsoring Executive	CFO/CIO	CEO/CRO
11. Supervising Manager	Operations Manager	Business Continuity Manager
12. Certifications	Ancillary	Numerous
13. Career Pathing	Limited	Broad

3. **Orientation:** The nature of disaster recovery is to restore technology-oriented services while business continuity focuses on the quick recovery of business oriented services. Technology-oriented services include voice and data networks, e-mail, and access to applications, databases and the Internet. Business-oriented services include safe and functioning facilities for critical office workers, vital hardcopy records they may need to transact business, and manual work-around procedures to sustain customer, supplier and revenue activities.
4. **Decade of Origin:** It is no coincidence that around the time companies began depending more on their IT departments and data centers for competitive advantage, they also realized the need to address disaster recovery of these same data centers. The decade of origin for this shift in emphasis was the 1970's. Mainframe computers were quickly becoming faster, cheaper and smaller; and the systems they hosted were becoming more critical than ever to the success of the business. By the late 1980's, the convergence of computers, communications and the Internet caused the tight integration of technical processes and business processes. Disaster recovery plans that focused only on technical recoveries were no longer adequate to sustain viable business operations. By the 1990's, the discipline of business continuity provided a more comprehensive, business-oriented approach to dealing with business disasters.
5. **Degree of Customer Involvement:** For this category, the term customers refers to the managers of end users who are not part of the IT department. These customers are in positions of authority, and can approve or disapprove of having their systems involved in disaster recovery exercises. The difference between disaster recovery and business continuity in terms of the degree of customer involvement is that the former has a minimal role because most of the recovery is of technical processes not business ones, while the latter has an extensive role because most all critical business processes are included in the planning and customers are generally the owners of these processes.
6. **Variety of Support Groups:** Disaster recovery planning, plans, and exercises utilize a relatively few number of support groups. Most of these support groups are within the IT department such as systems administrators, voice and data network administrators, database administrators and software developers. By comparison, business continuity planning involves a diverse set of support groups that include facilities, human resources, records management vendors, and in some cases public safety agencies such as police, fire, emergency medical and building inspectors.
7. **Number of Users Participating:** Disaster recovery and business continuity both involve the development of plans, the testing of those plans, and the

use of the plans during an actual disaster. One of the differences in these activities is that disaster recovery generally has no end users participating in any of these stages while business continuity has large numbers of business users (end-users) participating in all three of the stages. The reason for this is make the business continuity planning more complete, realistic, and likely to secure business unit buy-in.

8. **Primary Metrics:** The primary metrics for disaster recovery are similar to what is typically used for availability management: the mean time between failure (MTBF) and the mean time to recover (MTTR). MTBF is the average length of time between major outages usually measured in months. In the case of disaster recovery MTBF refers to the average time between disasters, or events, that cause major damage to a data center and sustained outages to critical computer services, and is typically measured in years. MTTR is the average time to restore computer services that have been interrupted and is usually measured in hours.

Business continuity uses recovery point objective (RPO) and recovery time objective (RTO) as its primary metrics. The RPO is the amount of data lost measured in time. For example, if you backup all of your critical data every night at midnight and then have a disaster at 1:00pm the next afternoon, all of the new data generated since the last backup is lost. If the RPO four hours then the data needs to be backed up every four hours to ensure no more than four hours of data is lost. The RTO is similar, but not identical, to the MTTR used in disaster recovery. The difference is that RTO is the maximum expected time by which service is expected to be restored, whereas MTTR is the elapsed recovery time averaged over a specified time period. In the past, most companies focused more on reducing RTO than RPO, emphasizing the quick restoration of service over lost data. But recently, with the advent of data mirroring and replication, many shops are devising their recovery strategies to minimize the RPO even if it means briefly extending the RTO.

9. **Management Style:** When managers in the past activated an IT disaster recovery plan, a major calamity had already occurred and caused impact. As a result, a more dictatorial, military style of management was usually employed. Immediate and orderly action was needed to assess damage, ensure the safety of life, limb and property, and to execute an effective recovery plan. With business continuity, comprehensive business and technical recovery plans are developed, tested and operationally exercised in a spirit of collaboration. When a disastrous event does occur, the lessons learned during exercises can be put to use to activate recovery with a more collaborative, supportive approach.
10. **Sponsoring Executive:** Prior to the era of business continuity plans, the executives responsible for IT disaster recovery were usually the CFO or the

CIO. Most of the planning and restoration activities focused on the recovery of the data center. As these activities gradually expanded to include business recovery across the enterprise, CEOs and Chief Risk Officers (CRO) become responsible. In several companies where I worked recently, the CRO is responsible for presenting a summary of business continuity recovery plans to the firm's board of directors. It's important to know that depending on the industry in which you work, your CEO or CRO may be liable for ensuring that viable business continuity plans exist and have been tested for the various business units.

11. **Supervising Manager:** Because IT disaster recovery used to pertain primarily to IT departments in general, and the data center in particular, it's easy to see why the Computer Operations was normally the supervising manager during a recovery scenario regardless of it being real or simulated. Business continuity by definition includes both business and technical recoveries and has the coordination of developing and testing plans centralized under business continuity manager. It should be noted that the Business continuity manager is not the supervising manager during an actual disaster within a particular business unit. In this case, the business unit manager would enact the recovery plan for his/her specific unit while the business continuity manager would provide coordination and communication among the business units and senior management.
12. **Certifications:** The field of IT disaster recovery has few recognized certification programs. At best there are ancillary certifications involving facilities management for data centers and emergency response certifications for secured facilities. Business continuity, on the other hand, has numerous certification programs such as those offered by the Disaster Recovery Institute for Certified Business Continuity Planner (CBCP) and Master Business Continuity Planner (MBCP). The Association of Contingency Planners (ACP) also sponsors certification programs.
13. **Career Pathing:** The difference in career pathing between disaster recovery and business continuity continues to widen. There are limited career paths for IT disaster recovery; one possibility is the link to logical and physical security. Business continuity continues to grow and prosper as a career path. The increasing frequency of natural disasters and especially the threat of terrorist activities have greatly heightened the awareness and value of business continuity programs.

The following is a list of physical and logical entities within an Information Technology environment which require the application of a Business Continuity Methodology. Applying the methodology should include the definition of things such as policies, guidelines, standards, procedures, etc., for each item in the list:

**Defining
Organization's
Business Continuity
Requirements**

- Frames and Managed Systems
- Firmware and Microcode
- Internal and external disk storage
- Frame or Managed System Names
- Partition Names
- Node Names
- Host Names
- DNS Aliases
- Hardware Management Consoles and Console Access
- Virtualization
- Networking Design
- VLAN's
- TCP/IP Subnets
- Resource or Service Groups
- Workload Management
- Volume Groups
- Logical Volumes / Disk Partitions
- Journaling Filesystems Log
- Filesystem mount points
- User names and UID numbers
- Group names and GID numbers
- Security
- High Availability
- System Installation
- Application Installation
- Database Installation
- System Monitoring
- Application Monitoring
- Database Monitoring
- Patch Management

Check Your Progress 4

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) What are the strategies of disaster Recovery?

.....

.....

.....

.....

2) List the differences Between Disaster Recovery and Business Continuity.

.....

.....

.....

.....

3) What should be the recovery time objective (RTO)

.....

.....

.....

.....

3.9 RISK AND RISK ASSESSMENT IN BUSINESS CONTINUITY

Business Continuity Management process within an organisation in order to mitigate the technology and information continuity risks identified as part of Risk Management.

In order to maintain availability of IT and information the organisation needs to understand

- which processes are critical;
- how quickly they must to be restored;
- what are the IT and information required in order to keep these critical processes running.

Risk is present in all decisions and activities undertaken by organisations and a number of these will present continuity issues. The approach to managing these continuity risks is twofold:

- 1 Pro-actively manage the risk, as part of the organisation's Risk Management process on an ongoing basis to lessen the likelihood or impact of an incident. The Business Continuity process itself can highlight further risks, which will themselves become part of the Risk Management process.

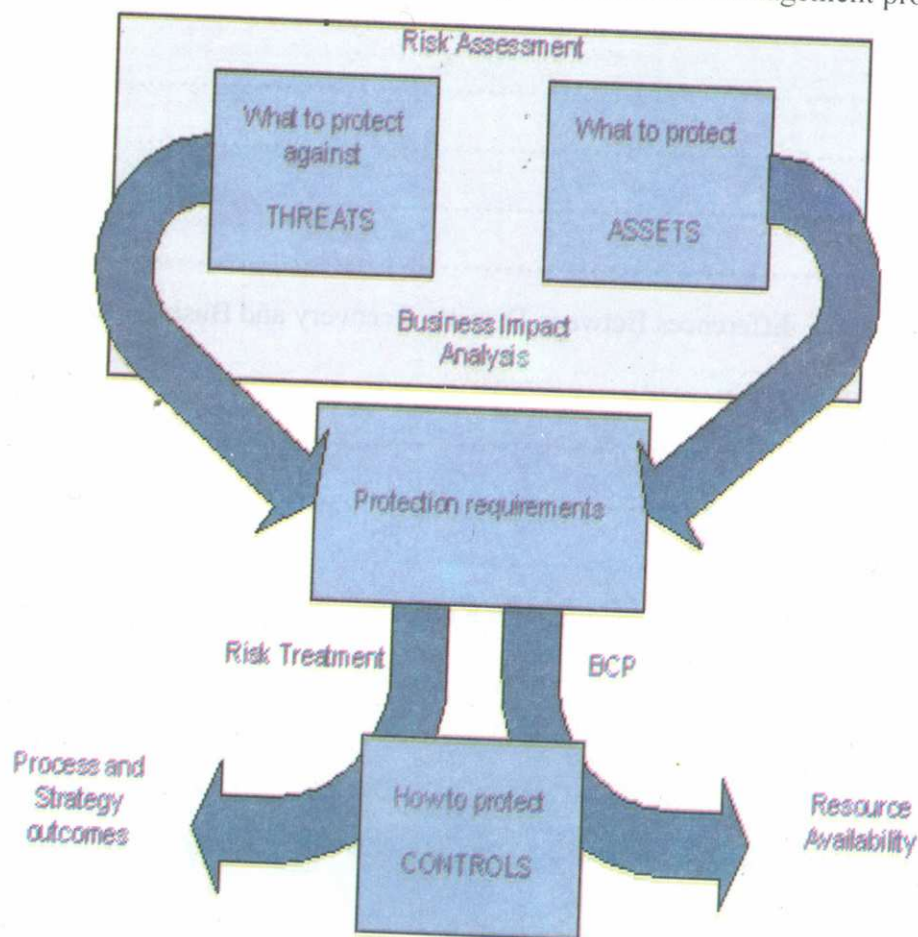


Fig. 4

2. Implement a Business Continuity Management process to treat residual risk. Business Continuity Management should be conducted as one of the required outcomes of the Risk Management programme. Business Continuity is one of the ways of modifying risk to lessen the impact if the risk occurs; especially in cases where avoiding, transferring or accepting the risk are not appropriate risk treatments. This could be considered a reactive method of managing risk.

ISO 27001:2005 calls for Business Continuity Management, as a method of risk treatment, to be considered as a measure to counteract interruptions to business activities and to protect critical business processes from the effect of major failures of information systems or disaster as well as to ensure their timely resumption

A further comparison of Risk Management and Business Continuity Management is given in the following table.

	Risk Management	Business Continuity Management
Key Method	Risk Analysis	Business Impact Analysis
Key Parameters	Impact and Probability	Availability and Impact
Type of incident	All types of events	Events causing significant business disruption
Size of events	All events affecting the organisation	Those threatening availability of organization's core processes
Scope	Focus primarily on management of risks to core business objectives, to prevent or reduce incidents	Focus mainly on incident management and recovery of critical business processes following an incident
Intensity	All, from gradual to sudden	Sudden or rapid events (although response may also be appropriate if a creeping incident suddenly becomes severe)

Business Continuity Management is concerned with managing risks to ensure that at all times an organization can continue operating at least to a pre-determined minimum level. The BCM process involves reducing the risk to an acceptable level and planning for the recovery of business processes should a risk materialise and a disruption to the business occur.

Disaster Recovery Planning is concerned with the actual technical recovery of the IT components and details the procedures to be used to restore the IT components following a failure.

Information Technology Service Continuity Management (ITSCM) ensures that information technology technical and services facilities (including computer systems, networks, applications, telecommunications, technical support and service desk – referred to as IT components throughout the remainder of this document) can be recovered within required and agreed business timescales. ITSC Management should be part of the overall BCP and not dealt with in isolation (PAS 77: 2006). The major difference between DR planning and ITSCM is that the user requirements drive ITSCM - their

recovery time objectives and agreed recovery sequence (taken from dependencies and RTO for applications). This enhances the service as it focuses the recovery effort on the Business Continuity requirements and reduces disruption to the critical processes.

Definitions of the various risk-related disciplines are given in the following table.

Risk discipline	Description
Corporate Governance	The system by which entities are directed and controlled [HB 254-2005]
Risk Management	Process of enhancing an organisation's likelihood of success in achieving its objectives [HB 254-2005], [BS 31100 DPC]
IT Risk Management	The process, distinct from Risk Assessment, of weighing policy alternatives for the safeguard of data assets and IT systems in consultation with interested parties, considering Risk Assessment and other legitimate factors, and selecting appropriate prevention and control options. (ENISA)
Business Continuity Management	BCM assures the availability of processes and resources in order to ensure the continued achievement of critical objectives [HB 293-2006]
IT Service Continuity Management	Supports the overall Business Continuity Management process by ensuring that the required information technology components can be recovered within required, and agreed, business timescales and in the agreed order of priority, from data extracted from the BIAs. The underlying recovery procedures can then be prioritised to effect recovery in a timely fashion [PAS 77]
Disaster Recovery Planning	Disaster Recovery Planning refers to an IT-focused plan designed to restore operability of the target system, application, or computer facility. The scope may overlap that of an IT Service Continuity Plan; however, the DR Plan is narrower in scope as it does not address the requirements of the business (based on [NIST])

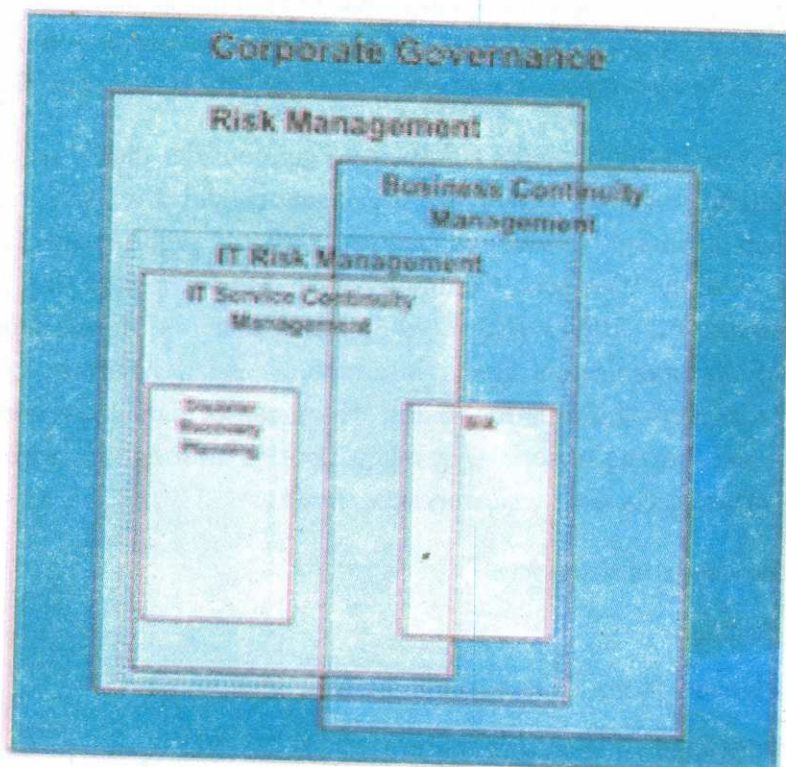


Fig. 5

The relationships among Corporate Governance, Risk Management, Business Continuity Management, IT Service Continuity Management and Disaster Recovery Planning are complex since some can exist without the others. The following figure tries to explain the relationships, should they co-exist.

BCM overlaps with Risk Management, and one of the areas of convergence is Business Impact Analysis. If ITSCM is in place, it utilises some of BIA's information in order to achieve Continuity Management and align it with the needs of the business. That is the only information which BCM and ITSCM have in common. ITSCM uses this information in order to prioritise the plans developed through DR Planning.

If ITSCM does not exist within the organisation then DR Planning is the proactive risk mitigation function of Risk Management and although it impacts BCM and can be invoked by a BCM event it is not part of BC. Similarly, ITSCM can exist without BCM but requires a subset of BIA information so the Business must conduct BIAs in order to ascertain the necessary information. If there are no DR Plans then these must also be developed. DR Planning is an essential part of ITSCM. Although it may not exist when originally developed it must be in operative if ITSCM is to be considered complete. In a similar way, BCM cannot exist without BIA information.

Risk Management and Business Continuity need to be considered as an integrated whole together with IT Service Continuity and Information Security. The successful implementation of a robust Business Continuity Plan is

dependent upon having a tried and tested ITSC Plan in place which improves the technological resilience of the organisation. This requires the presence of procedures for restoration should any part of the IT infrastructure fail.

Not only should the Business Continuity Plan consider the IT requirements of the business processes within the organisation, and how ICT will organise themselves to restore services to meet the business requirements following an incident, but the Business Continuity Plan must consider the information requirements. BS 7799-3 [BS 7799-3] states that one of the most valuable assets of an organisation is its information which needs to be protected whatever its form. Information assets, which can be databases, contracts, user manuals and training materials, or other types of information, are stored on or used by other assets and these, may be defined as:

- Processes and services
- Software
- Physical items
- Personnel

Information Security (IS) must be able to recover its own processes following

An incident in order to be able to restore the business processes information requirements. Interdependencies will exist between ICT and IS and the two will need to work together to ensure an integrated approach which meets business needs:

There are other security disciplines related to Business Continuity which are described in the following paragraphs and illustrated below.

Emergency Planning: Emergency planning is a process resulting in a set of agreed procedures to prevent, reduce, control, mitigate and take other actions in the event of a civil emergency which impacts the organisation [BS 25999-1].

Incident Response: Incident response is the immediate response to an incident usually within the first few hours of occurrence. It is an important phase in which control should be gained of the incident, the impact assessed, personnel made safe and key communications made to staff, public, stakeholders and the media. If control is not gained at this stage it is extremely difficult to implement effective incident management thereafter (Glen Abbot).

Incident Management: Incident Management is the process of taking central command and control of an incident which threatens the operations, staff, stakeholders or reputation of an organisation. The incident management team ensures that staffs are able to restart their critical processes and communications are made internally and externally (Glen Abbot).

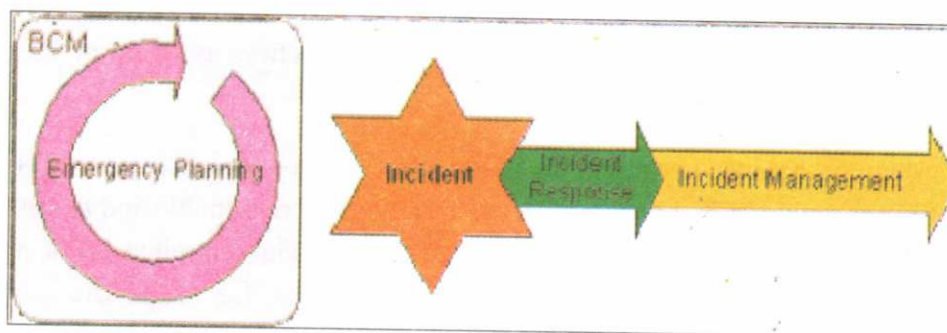


Fig. 6

Check Your Progress 5

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

- 1) Explain the difference between Risk management and business continuity management.

.....

.....

.....

.....

- 2) Explain the relationships among Corporate Governance, Risk Management, Business Continuity Management, IT Service Continuity Management and Disaster Recovery Planning.

.....

.....

.....

.....

- 3) What are the approaches to manage business continuity risks?

.....

.....

.....

.....

3.10 LET US SUM UP

Information security controls can be classified as physical, technical, or administrative. These are further divided into preventive and detective controls. The organization's security policy should be reviewed to determine the confidentiality, integrity, and availability needs of the organization. The

appropriate physical, technical, and administrative controls can then be selected to provide the required level of information protection, as stated in the security policy.

A careful balance between preventive and detective control measures is needed to ensure that users consider the security controls reasonable and to ensure that the controls do not overly inhibit productivity. The combination of physical, technical, and administrative controls best suited for a specific computing environment can be identified by completing a quantitative risk analysis. Because this is usually an expensive, tedious, and subjective process, however, an alternative approach — referred to as meeting the standard of due care — is often used. Controls that meet a standard of due care are those that would be considered prudent by most organizations in similar circumstances or environments. Controls that meet the standard of due care generally are readily available for a reasonable cost and support the security policy of the organization; they include, at the least, controls that provide individual accountability, audit ability and separation of duties.

An often overlooked issue in information security involves human users. To protect your organization, it is essential that an Information Security Plan be included as part of the plans to address the resiliency of the organization. This plan should include a broad range of security issues such as how individuals interact with computers, policies for laptop use, and the access and authorities needed to do their jobs. Business continuity professionals should collaborate with information security professionals to raise awareness of security and to provide training for all employees with the goal to reduce the risks to the organization.

3.11 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

- 1) Some common threats to the business continuity are the following:

Security, Earthquake, Fire, Flood, Cyber attack, Sabotage (insider or external threat), Hurricane or other major storm, Utility outage, Terrorism, Theft (insider or external threat, vital information or material), Random failure of mission-critical systems.

- 2) There are different threats to an organization.

- (i) Security threats to an organization

- a. Malicious Internet Content
- b. Attacks on physical Systems
- c. Authentication and privilege attacks

d. Denial of services

(ii) Impact of information technology threats

- 3) Passwords are the main authentication and privilege attack in an organization. It is not an easy task to have a secure system whereby people are required to choose a unique password that others cannot guess but is still easy for them to remember. Nowadays most people have at least five other passwords to remember, and the password used for company business should not be the same one used for webmail accounts, site memberships and so on. Password policies can go a long way to mitigate the risk, but if the password policy is too strict people will find ways and means to get around it. They will write the password on sticky notes, share them with their colleagues or simply find a keyboard pattern (1q2w3e4r5t) that is easy to remember but also easy to guess. Most complex password policies can be easily rendered useless by non-technological means.

In Organizations another authentication problem is the access rights, with full access privileges, a systems administrator may plan a logic bomb, backdoor accounts or leak sensitive company information that may greatly affect the stability and reputation of the organization.

4) Requirements of the business Continuity are as follows

- Maintain a continuous flow of your business operations under virtually any condition
- Assess Design and Plan for a resilient business infrastructure.
- Protect and Recover vital business information.
- Fault tolerant, failure resistant IT infrastructure.
- Ensure high availability of IT infrastructure.
- Identify and integrate critical business and IT priorities into a comprehensive continuity and resiliency program.
- Risk assessment and integrated risk management services ensure secure IT operations and safety of data.
- Processes designed keeping in mind dynamic business requirements.

Check Your Progress 2

- 1) **Security** is generally defined as the freedom from danger or as the condition of safety. Computer security, specifically, is the protection of data in a system against unauthorized disclosure, modification, or destruction and protection of the computer system itself against unauthorized use, modification, or denial of service. Because certain computer security controls inhibit productivity, security is typically a

compromise toward which security practitioners, system users, and system operations and administrative personnel work to achieve a satisfactory balance between security and productivity.

- 2) Controls for providing information security can be physical, technical, or administrative. These three categories of controls can be further classified as either **preventive or detective**. Preventive controls attempt to avoid the occurrence of unwanted events, whereas detective controls attempt to identify unwanted events after they have occurred. Preventive controls inhibit the free use of computing resources and therefore can be applied only to the degree that the users are willing to accept. Effective security awareness programs can help increase users' level of tolerance for preventive controls by helping them understand how such controls enable them to trust their computing systems. Common detective controls include audit trails, intrusion detection methods, and checksums.

Three other types of controls supplement preventive and detective controls. They are usually described as **deterrent, corrective, and recovery**.

Deterrent controls are intended to discourage individuals from intentionally violating information security policies or procedures. These usually take the form of constraints that make it difficult or undesirable to perform unauthorized activities or threats of consequences that influence a potential intruder to not violate security (e.g., threats ranging from embarrassment to severe punishment).

Corrective controls either remedy the circumstances that allowed the unauthorized activity or return conditions to what they were before the violation. Execution of corrective controls could result in changes to existing physical, technical, and administrative controls.

Recovery controls restore lost computing resources or capabilities and help the organization recover monetary losses caused by a security violation.

- 3) Preventive controls attempt to avoid the occurrence of unwanted events, whereas detective controls attempt to identify unwanted events after they have occurred. Preventive controls inhibit the free use of computing resources and therefore can be applied only to the degree that the users are willing to accept. Effective security awareness programs can help increase users' level of tolerance for preventive controls by helping them understand how such controls enable them to trust their computing systems. Common detective controls include audit trails, intrusion detection methods, and checksums.
- 4) Physical Controls - is the use of locks, security guards, badges, alarms, and similar measures to control access to computers, related equipment

(including utilities), and the processing facility itself. In addition, measures are required for protecting computers, related equipment, and their contents from espionage, theft, and destruction or damage by accident, fire, or natural disaster (e.g., floods and earthquakes).

a. Preventive

- i. Backup Files and documentation
- ii. Fences
- iii. Security Guards
- iv. Badge Systems
- v. Double door systems
- vi. Locks and Keys
- vii. Backup Power
- viii. Biometric Access Controls
- ix. Site selection
- x. Fire Extinguishers

b. Detective

- i. Motion Detectors
- ii. Fire and Smoke Detectors
- iii. Closed circuit Television Monitors
- iv. Sensors and Alarms

Technical Controls - involves the use of safeguards incorporated in computer hardware, operations or applications software, communications hardware and software, and related devices. Technical controls are sometimes referred to as logical controls.

a) Preventive

- i. Access control software
- ii. Antivirus software
- iii. Library Control system
- iv. Passwords
- v. Smart Cards
- vi. Encryption
- vii. Dial-up access control and callback systems

b) Detective

- i. Audit Trails
- ii. Intrusion Detection Systems

Administrative Controls or personnel, security consists of management constraints, operational procedures, accountability procedures, and supplemental administrative controls established to provide an acceptable level of protection for computing resources. In addition, administrative controls include procedures established to ensure that all personnel who have access to computing resources have the required authorizations and appropriate security clearances.

a) Preventive

- i. Security Awareness and Technical Training
- ii. Separation of duties
- iii. Recruitment and termination procedures
- iv. Security policies and procedures
- v. Supervision
- vi. Disaster recovery , contingency and emergency plans
- vii. User registration for computer access

b) Detective

- i. Security reviews and Audits
- ii. Performance evaluations
- iii. Required vacations
- iv. Background investigation
- v. Rotation of duties

Check Your Progress 3

- 1) Over the last few years, every business has faced an onslaught of challenges: global economic volatility, fierce competition, customer churn, mergers and acquisitions, rising security concerns and waves of regulatory compliance issues. Meanwhile, stakeholders continue to demand that top executives increase profits, lower costs, expand market share and grow revenue. To solve these issues, much has been demanded from your information technology infrastructure.

You depend on IT to keep the business running, to harness complex, often competing, initiatives into a larger, strategic vision that supports the business. Most importantly, you need the resilient information and

applications, systems and security that can support the business wherever the future leads it.

- 2) Information resilience encompasses most of the data, applications and systems aspects of what we know as business continuity, continuous availability, high availability, and data protection and recovery. Information resilience looks at the long-term viability of the IT “dial tone” that runs your business today, tomorrow and long into the future.

Because a business thrives on information, the availability of that information plays a key role in business resilience. Any interruption or interference (downtime) that makes your information or applications inaccessible or inaccurate adds delay to your go-to-market processes, supply chain, analyses and every day, even vital, decisions.

Downtime prevents immediate action from your customers, employees and business partners. Many business executives are not even aware of this built-in hidden, but altogether unnecessary cost. A truly resilient business, however, will take steps to solve downtime issues throughout all of its business processes and in its IT infrastructure.

- 3) Traditionally, the focus of Information Security efforts has centered on virus detection and prevention, hacking into systems and securing networks from unintended intrusions.

While these are still admirable areas to work on and provide measurable goals for internal reporting, they are just the tip of the iceberg. The weakest links in our information security protocols are employees.

People are a critical factor in ensuring the security of computer systems and information resources. Information security needs to begin on the desk PC or the laptop that travels between work and home. The role of the business continuity professional is to be aware of threats, make all employees aware of threats, and to work with the information security professionals to ensure that policies and procedures are in place to protect the organization.

- 4) While some unplanned downtime results from weather or other disaster, most happens because of hardware or application failures, human errors and security violations. Surprisingly though, studies show that planned interruptions (downtime) caused by routine daily/weekly backups, system upgrades, performance tuning and batch jobs create 70-90 percent of interruptions for most businesses.

Check Your Progress 4

- 1) Prior to selecting a disaster recovery strategy, a disaster recovery planner should refer to their organization's business continuity plan which should indicate the key metrics of recovery point objective (RPO) and recovery

time objectives (RTO) for various business processes (such as the process to run payroll, generate an order, etc.). The metrics specified for the business processes must then be mapped to the underlying IT systems and infrastructure that support those processes.

- **Recovery point objective (RPO)** describes the acceptable amount of data loss measured in time.

The recovery point objective is the point in time to which you must recover data as defined by your organization. This is generally a definition of what an organization determines is an "acceptable loss" in a disaster situation. The RPO allows an organization to define a window of time before a disaster during which data may be lost. The value of the data in this window can then be weighed against the cost of the additional disaster prevention or loss-prevention measures that would be necessary to close the window.

- The **recovery time objective (RTO)** is the duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity. It includes the time for trying to fix the problem without a recovery, the recovery itself, tests and the communication to the users. Decision time for users representative is not included. The business continuity timeline usually runs parallel with an incident management timeline and may start at the same, or different, points.

2) There are 13 differences between disaster recovery and business continuity.

Category	Disaster Recovery	Business Continuity
1. Area of Emphasis	Data Center	Enterprise
2. Approach	Reactive	Proactive
3. Orientation	Technology	Business
4. Decade of Origin	1970's	1990's
5. Degree of Customer Involvement	Minimal	Extensive
6. Variety of Support Groups	Few	Diverse
7. Number of Users Participating	None	Many
8. Primary Metrics	MTBF/MTTR	RPO/PTO
9. Management Style	Dictatorial	Collaborative
10. Sponsoring Executive	CFO/CIO	CEO/CRO
11. Supervising Manager	Operations Manager	Business Continuity Manager
12. Certifications	Ancillary	Numerous
13. Career Pathing	Limited	Broad

- 3) The **recovery time objective (RTO)** is the duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in continuity. It includes the time for trying to fix the problem without a recovery, the recovery itself, tests and the communication to the users. Decision time for users representative is not included.

The business continuity timeline usually runs parallel with an incident management timeline and may start at the same, or different, points. In accepted business continuity planning methodology the RTO is established during the Business Impact Analysis (BIA) by the owner of a process (usually in conjunction with the business continuity planner). The RTOs are then presented to senior management for acceptance.

The RTO attaches to the business process and not the resources required to support the process. The RTO and the results of the BIA in its entirety provide the basis for identifying and analyzing viable strategies for inclusion in the business continuity plan. Viable strategy options would include any which would enable resumption of a business process in a time frame at or near the RTO. This would include alternate or manual workaround procedures and would not necessarily require computer systems to meet the RTOs

Check Your Progress 5

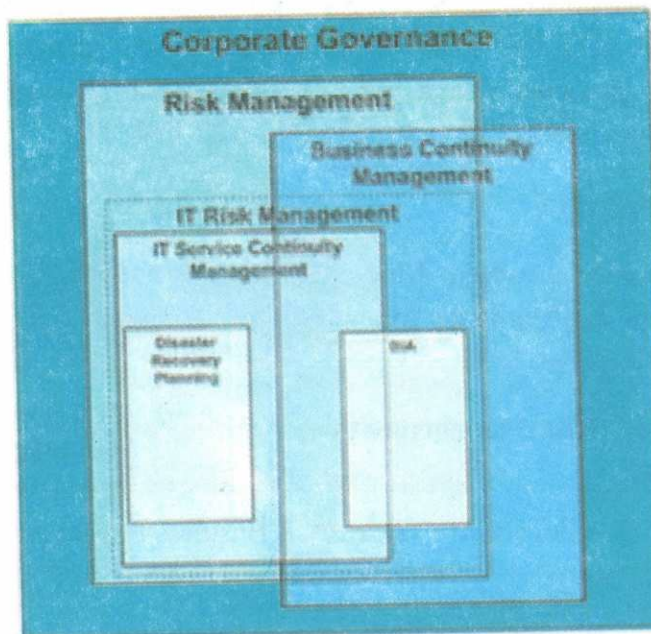
- 1) The difference between Risk management and business continuity management is given in the following table.

	Risk Management	Business Continuity Management
Key Method	Risk Analysis	Business Impact Analysis
Key Parameters	Impact and Probability	Availability and Impact
Type of incident	All types of events	Events causing significant business disruption
Size of events	All events affecting the organisation	Those threatening availability of organisation's core processes
Scope	Focus primarily on management of risks to core business objectives, to prevent or reduce incidents	Focus mainly on incident management and recovery of critical business processes following an incident

Intensity	All, from gradual to sudden	Sudden or rapid events (although response may also be appropriate if a creeping incident suddenly becomes severe)
------------------	-----------------------------	---

- 2) The relationships among Corporate Governance, Risk Management, Business Continuity Management, IT Service Continuity Management and Disaster Recovery Planning are complex since some can exist without the others. The following figure tries to explain the relationships, should they co-exist.

BCM overlaps with Risk Management, and one of the areas of convergence is Business Impact Analysis. If ITSCM is in place, it utilises some of BIA's information in order to achieve Continuity Management and align it with the needs of the business. That is the only information which BCM and ITSCM have in common. ITSCM uses this information in order to priorities the plans developed through DR Planning.



- 3) There are other security disciplines related to Business Continuity which are described in the following paragraphs and illustrated below.

Emergency Planning: Emergency planning is a process resulting in a set of agreed procedures to prevent, reduce, control, mitigate and take other actions in the event of a civil emergency which impacts the organisation [BS 25999-1].

Incident Response: Incident response is the immediate response to an incident usually within the first few hours of occurrence. It is an important phase in which control should be gained of the incident, the impact assessed, personnel made safe and key communications made to staff,

public, stakeholders and the media. If control is not gained at this stage it is extremely difficult to implement effective incident management thereafter (Glen Abbot).

Incident Management: Incident Management is the process of taking central command and control of an incident which threatens the operations, staff, stakeholders or reputation of an organisation. The incident management team ensures that staffs are able to restart their critical processes and communications are made internally and externally (Glen Abbot).

3.12 SUGGESTED READINGS

- BusinesscontinuityToday.com
- IT Management Reference Guide, hosted by Rich Schiesser

UNIT 4 IDENTIFYING AND SELECTING BUSINESS CONTINUITY STRATEGIES

Structure

- 4.0 Introduction
- 4.1 Objectives
- 4.2 Purpose of Business Continuity Strategy
- 4.3 Define Business Continuity Strategy
- 4.4 Selection of Business Continuity Strategy
- 4.5 Business Continuity Planning in IT
- 4.6 Determining Strategies
- 4.7 Determining Business Continuity Management Strategies
- 4.8 Let Us Sum Up
- 4.9 Check Your Progress: The Key
- 4.10 Suggested Readings

4.0 INTRODUCTION

The strategy identification process should address threats to and the loss of key facilities, key people, equipments, technologies and business partners. This process should take into account the results from the risk assessment and business impact analysis so that the strategy selection assumptions are valid and realistic. For example, the risk assessment, together with the strategy identification methodology, helps to define what an appropriate distance may be between primary and alternate facilities.

An effective Business Continuity strategy is typically two-fold. It includes risk reduction activities to take place before an interruption occurs, as well as response activities to mitigate impact when it does. Business Continuity professionals have the task of allocating their limited resources, in the most efficient way possible, to achieve maximum risk and impact reduction. This task can appear daunting when considering a company with a wide variety of business areas. To simplify the resource allocation decision both before and after a crisis, it is helpful to have a defined framework in which to organize and evaluate information. A framework not only allows the professional to assess existing information, but also makes it possible to quickly incorporate new information into their assessment so that areas can be re-evaluated during an interruption and an effective recovery strategy can be developed.

At first glance, the decision of which areas to allocate the most resources to seems simple - identify the areas that are most important to the financial health

of the business and invest the most to protect and recover those. However, when a company has many areas that are relatively similar in criticality, this logic may not truly capture the information necessary to make the best decisions. Additionally, criticality may be hard to measure; for example, the potential impact on the company for product lines in their beginning stages is difficult to predict.

A large manufacturer faced this problem. The organization has considerable assets distributed over a large number of different product lines and because they value the safety of their customers most, they know that they can't evaluate criticality alone. To emphasize this point, some of the newer programs that may contribute the most to their future business success are still in the research phase and thus are not generating revenue. The organization wants an efficient prioritization of products that will minimize the impact of an interruption on both present and future revenues, while also minimizing the impact to the customer. Effectively, they want a recovery order that effectively allocates business continuity resources and can be continually modified to incorporate new information. After much consideration, management has decided to add an additional characteristic to evaluate each product line: recoverability. This is a measure of the amount of resources it takes to recover following an interruption.

For example, an area high in criticality but also high in recoverability difficulty does not justify as much effort towards risk reduction as an area at mid-level criticality with low recoverability difficulty. In the same line of thought, an area that is high in criticality but low in recoverability difficulty will be targeted for protection immediately following a crisis, while an area also high in criticality but easily recoverable will not be focused on initially. Without the matrix, these conclusions would be hard to reach in a stressful situation.

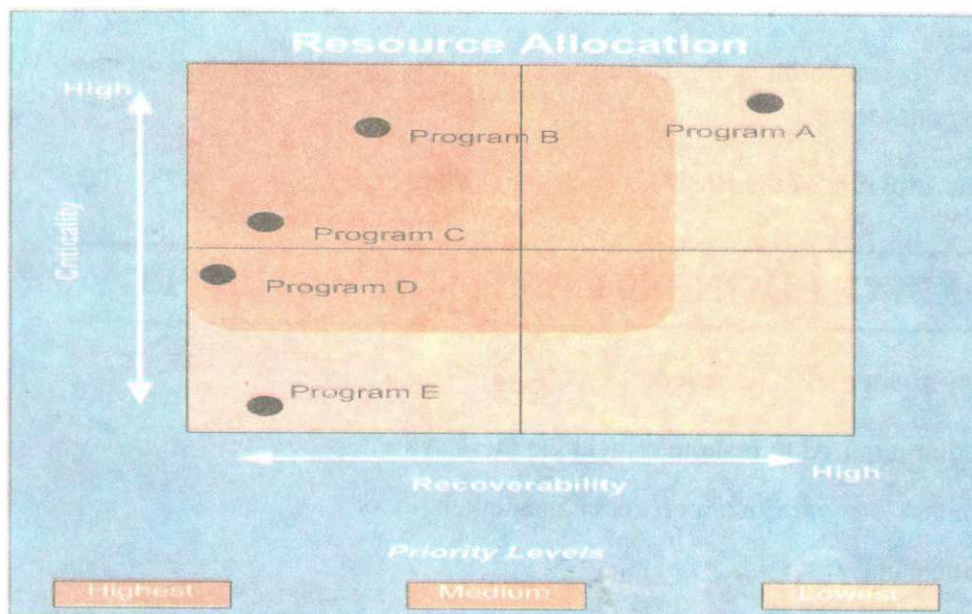


Fig. 1

4.1 OBJECTIVES

After studying this unit, you should be able to understand:

- purpose of business continuity strategy;
- definition of business continuity strategy;
- selection strategy of business continuity;
- business continuity planning in IT;
- determining strategies; and
- determining Business continuation management strategies.

4.2 PURPOSE OF BUSINESS CONTINUITY STRATEGY

The purpose of the Business Continuity Strategy is to agree the priorities for recovery and to identify the resources that will be used to recover the business. Business Continuity strategy development should addresses:

- The implementation of measures to increase the resilience of the organization to mitigate the impact of an incident.
- The use of alternative arrangements such as home or remote working or alternative office accommodation.
- The agreed recovery objectives those are achievable with the resources available.
- The responsibilities for Business Continuity and the structure of the response teams.
- The structure of the Business Continuity Plans.

4.3 DEFINE BUSINESS CONTINUITY STRATEGY

Continuity strategies may include:

- action required to resume critical business activities
- contact lists of critical personnel and stakeholders
- counseling
- critical business activities and prioritisation of when they can/need to resume

- list of resources

Once your key activities and resources have been identified together with the associated risks, now it is important to decide that how you will manage these risks. The following lists of strategies are commonly applied:

- Accept the risks and change nothing
- Attempt to reduce the risks
- Attempt to reduce the risks and make plans to restore key activities as soon as possible
- Cease the activity altogether

All of these approaches will need a detailed plan outlining the arrangements for the incident. You should also consider how quickly recovery would need to take place for the strategic areas of your business or various departments.

It may be useful to draw a chart of the timescales involved in re-establishing certain functions.

One essential decision is how you respond to risks that cannot be reduced.

4.4 SELECTION OF BUSINESS CONTINUITY STRATEGY

The risk analysis and business impact analysis have identified risks to key business functions. Also, the potential impacts and probabilities of these risks as well as the costs to prevent or mitigate damages and the time to recover will have been established. Evaluating and selecting strategies is based on using this knowledge. Strategy selection involves focusing on key risk areas and selecting a strategy for each one. The primary goals are to maintain business continuity in the face of a disruption or disaster to recover, to key business functions quickly and to mitigate damages.

Many companies associate disaster recovery and business continuity only with IT and communications functions and miss other critical areas that can seriously impact their business. Other common areas for strategy development and selection are employees, facilities, power, customer service, billing, and customer and public relations. All areas require a very well planned strategy based on recovery time objectives cost and profitability impact.

Recovery related to employees is the most overlooked part of strategy selection. Simple steps like the ability to contact employees at home or on their personal cell phone and to ensure all are accounted for at each facility are often overlooked. Communications is critical to keep employees informed and engaged. The most powerful tools for continuity and recovery are the knowledge capabilities and motivation of employees.

Developing strategies with implementation steps means no time is wasted in a recovery scenario. The focus is to implement the plan quickly and successfully. The right strategies implemented effectively minimizes the disruption and mitigates damages.

In some cases, a strategy decision may be no strategy at all. In this scenario and others where there is significant risk to the financial viability of the organization, business interruption or business income insurance may be a viable strategy. Generally, this provides the company with the income it is losing due to damage to its property. It therefore increases the company's chances of survival and the ability to keep its customers and recover.

Determining Business Continuity Strategy

- Identifying and Selecting Strategies
- Identifying and Selecting Tactical Responses
- Consolidating Resource Levels

Strategy Development

- Establishing the 'worst case' scenario, and all 'less than worst case' scenarios, for which strategies need to be developed
- Identifying potential short term contingency strategies, and longer term recovery strategies, for critical business processes
- Determining order-of-magnitude costs and evaluating the relative merits for each strategy
- Selecting the preferred strategies and preparing cost justifications
- Implementing the approved strategies

Successful Strategies for Business Continuity Planning

Identifying and selecting Business Continuity strategies for:

- Mitigating risk
- Reducing impact
- Recovering computer systems
- Resuming business operations

4.5 BUSINESS CONTINUITY PLANNING IN IT

Key steps in developing a business continuity plan

The Business Continuity Institute's 'Business Continuity Management Life Cycle' model covers five key stages in developing and maintaining a business continuity plan.

Understanding your business

- Project initiation and management - get support from senior managers. Establish a management structure to develop and carry out the plan.
- Risk evaluation and control - identify the threats and the best defence. For example, with e-commerce, computer viruses might be a major threat - the appropriate defence might be regularly updated anti-virus software.
- Business impact analysis- establishes your business' critical processes and identifies the impact of any failures. For example, if your e-commerce website is critical to your operation, what would it cost your business if it went down for 24 hours?

Business continuity management strategies

- Develop an organizational business continuity strategy, identifying which areas you need to concentrate on. Focus on the critical operating requirements of the business, as identified above.
- Develop a process-level strategy - a documented framework clearly stating how critical processes will be restarted following an incident or failure. For example, if the payment system for your e-commerce website goes down, you need a specific strategy for resuming operations.

Developing and implementing a business continuity response

- Emergency response and operations - establish a crisis management process to respond to incidents.
- Develop and implement a business continuity plan. This describes specifically how you will deal with incidents. Focus on the priorities of your overall business continuity strategy.
- Put in place business unit plans for each department. For example, detail the actions that the IT department will have to carry out if IT services are lost.

Developing a business continuity management culture

- Awareness and training plans - ensure all staff are aware of the importance of business continuity and can operate effectively following an incident.
- Review the effectiveness of awareness training periodically. Identify any further training needed.

Exercising, maintenance and audit

- Test the business continuity plans. Test any technical aspects - for example if you plan to use backed-up data to restore operations. Carry out full live exercises to establish how the plans work in a disaster situation.
- Maintain the plans - ensure that the documentation remains accurate and reflects any changes inside or outside the business.
- Regularly audit the plans - do they meet the needs of your strategy? Act on your findings.

4.6 DETERMINING STRATEGIES

Business continuity is the process of preparing to ensure that critical business functions will be available in the event of disruptions to operations and/or key personnel. According to the Federal Financial Institutions Examination Council, a business continuity plan is essential for the purpose of helping a company to resume normal business activity in the event of a disaster by establishing backup systems and guidelines for emergency responses.

Personnel Strategies

- Personnel policies and decisions are a key component of a business continuity strategy. In order for a continuity plan to be effective, it must clearly designate the company's decision-making hierarchy in the event that important members of the management team are unavailable. There must be a notification process for informing the replacement management team of their new responsibilities. In addition, a business should have a plan in place for staying in contact with all of its employees regarding changes and situations that require attention and adjustments to typical working arrangements. This plan should also designate a staff member responsible for informing clients and vendors of changes that affect the company's relationship with them.

Emergency Planning

- Business continuity strategies address issues that may arise in the event of an emergency, so they should contain provisions designating protocols and policies for coping with crises. If a company's staff has a thorough understanding of the difficulties that may arise and the measures that they are expected to take, they are more likely to remain calm under pressure and make thoughtful, prudent decisions. In addition to verbally communicating expectations, a company's continuity training program should also involve practices and enactments of potential emergency scenarios.

- Because so many businesses depend on a technological infrastructure, a continuity plan should include strategies for ongoing access to data in the event of an emergency. Specific personnel should be assigned the responsibility of backing up files on a regular basis. An effective technological continuity strategy takes into account each element of a system and its relationship to the other components. For example, employees who operate at individual work stations must have access to the unique data that they input and maintain, and they must also have strategies for logging onto a company system in order to access shared information. In addition, continuity strategists should analyze the company's information system as a whole, identifying critical components such as channels for communicating with clients and vendors.

Based on your business requirements, recovery needs, and the tools that you have selected, determine and document the backup and recovery strategies for your environment.

For example, in an environment that has databases that are managed by DBAs, the strategies in the following list might be employed:

- All databases are backed up by SQL Server. The backup interval that is set is based on the following:
 - The importance of the content or service.
 - The effect on performance that the backup has on the environment.
- Small, quickly changing, very high-business-affect content databases are additionally protected by SQL Server database snapshots that are stored on a separate physical disk. Only one snapshot is stored per database, and snapshots are discarded regularly so that the effect on performance is minimized. The snapshot interval that is set for each database is based on the following:
 - The importance of the content or service.
 - The standard rate of change for the database.
 - The effect on performance that the snapshot has on the environment.
 - The amount of space that is required to store the snapshot.

Recovering from a snapshot is faster than standard recovery.

However, creating snapshots can decrease the performance of the underlying database. We recommend that the effect that snapshots have on the performance of the system be tested before they are implemented, and that snapshots be discarded regularly to reduce the space that is required.

4.7 DETERMINING BUSINESS CONTINUITY MANAGEMENT STRATEGIES

Determining and selecting Business Continuity Management Strategies to be used to maintain the organization's business activities and processes through an interruption.

Business Continuity Management Strategies concern:

- The selection of alternative operating methods to be used after an interruption to maintain or resume the organization's business activities and their dependencies (internal and external) to a priority, and time table determined in the Business Impact Analysis.
- The protection of vulnerable and single points of failure in business critical processes identified in the Risk Analysis

Strategies for Success

Designing and refining the organizational plan is critical to the success of continuity assurance. Unlike other documents, which are created once and can serve as an ongoing reference standard, the business continuity plan is a living document. Created by a process of internal assessment of business processes and resources, in order to remain useful, the plan must be reviewed and updated as conditions change.

Duplicate and Disperse

Beyond planning, a corporation's continuity strategy must incorporate specific hardware and software products. Because many vendors build products based on specific continuity strategies, buyers should understand how they mesh with the corporation's continuity plans. For example, some storage and backup technologies support the strategy known as "duplicate and disperse." This strategy encourages corporations to duplicate data so that it is available in geographically dispersed locations. In the event that one location or even region is inaccessible, data can be accessed at another location.

Selecting Software

Software products in the BCP market generally handle either continuity plan development or business impact analysis. When selecting a planning solution, buyers should look for a complete package that includes a powerful relational database. The database stores not only the plan document, but also any links to business processes, organizational departments and vendors mentioned in the plan. This is critical for keeping the plan current and establishing effective change control.

When choosing one of these products, investigate the expertise of the software vendor and the vendor's development team. Some handle continuity concerns only as a sideline to other business issues; others have only recently entered the continuity market. Certain vendors can provide only one type of software, while others offer integrated suites backed up by consulting services.

Consulting with Experts

Clearly, the rising stakes for business continuity will encourage many organizations to engage outside expertise. Consulting services are broad, and include education, business impact analysis, building and maintaining a plan, and risk analysis. Some consultants specialize in discrete aspects of the BCP market—such as testing the continuity plan or handling crisis communications—while other organizations are deep enough to address a wide range of continuity issues. Look for consultants who are certified BCP professionals, preferably those with at least five years of experience. Many talented continuity professionals have backgrounds in the military, the public sector, and law enforcement. To handle cross-enterprise continuity concerns, seek a consultancy with a broad portfolio of expertise.

Consider an organization with front-line experience, staffers who have been through real crises, as well as those with organizational development skills and focused disaster recovery-planning capabilities. Consultants who understand change control, have executive and managerial experience, possess an IT background, or have worked on total quality or process improvement initiatives can also be beneficial. Experts with strength in customer service can be especially valuable, since ongoing communications, requests and solutions are common in resolving continuity issues.

The Human Touch

In continuity planning, beyond all of the products and services, executives must factor in the most important asset of the business—its people. One critical element of this planning is crisis communications. When even the unimaginable happens, the executive team must be prepared to communicate realities, plans and actions to a variety of audiences—including employees, business partners, stakeholders, the media and the surrounding community. Every message communicated during a crisis must consider the human needs of the audience—even if the audience is varied. Regardless of the high-stakes situation, employees need to feel safe, stockholders want to hear how the company is protecting their investments, and a corporation's neighbors need proof that the business is acting in the best interests of the community. And although executives cannot anticipate every contingency, they can develop communications plans that address broad types of scenarios and define the corporate spokespeople, audiences and messages needed to recreate order from chaos.

Executive Engagement

To protect the enterprise most effectively, these three approaches are used in concert. Yet a full-blown BCP program requires executive commitment to ensure that the corporation is prepared to deal with any eventuality, and this can be costly

Choosing Wisely

Within the broad category of BCP are three discrete approaches to protecting against unpredictable business threats: continuity planning, recovery preparedness and risk management. Continuity planning addresses the steps taken to minimize the impact of uncontrollable conditions, such as installing generators to handle basic, short-term or emergency electrical needs during a power outage. Recovery preparedness covers the issues that can help an organization recover from crisis conditions, such as engaging a hot site where mirrored computer processes can run, should the home facility become inaccessible. Risk management reduces the likelihood of potential crises by taking steps such as training employees how to work safely, changing processes to reduce injury or implementing protective devices such as smoke detectors. Risk management can also include insuring the corporation against loss with policies that can protect against everything from physical damage to data loss and e-commerce breaches.

Recovery related to employees is the most overlooked part of strategy selection. Simple steps like the ability to contact employees at home or on their personal cell phone and to ensure all are accounted for at each facility are often overlooked. Communications is critical to keep employees informed and engaged. The most powerful tools for continuity and recovery are the knowledge, capabilities and motivation of employees.

Developing strategies with implementation steps means no time is wasted in a recovery scenario. The focus is to implement the plan quickly and successfully. The right strategies implemented effectively minimizes disruption and mitigation damages.

In some cases, a strategy decision may be no strategy at all. In this scenario, and others where there is significant risk to the financial viability of the organization, business interruption or business income insurance may be a viable strategy. Generally, this provides the company with the income it is losing due to damage to its property. It therefore increases the company's chances of survival and the ability to keep its customers and recover.

The strategy selection prompts a number of potential actions:

- Risk treatment decisions
- Engaging with third parties to set up contract

- Commitment to developing plans to deliver the selected strategies and tactical options

Your continuity plan must fit the needs of your organization. Here are just some of the services that your business continuity solution should provide:

- Business Impact Analysis and Risk Analysis to protect the most profitable segments of your business.
- Resource Dependency Analysis to identify the processes and applications critical to the organization's business continuity.
- Identifying and selecting appropriate and cost effective business continuity strategies.
- Developing user friendly and maintainable business continuity plans.
- Diverse options for testing continuity plans to confirm they are effective and build confidence in their use.
- Assessment of external third party continuity risks or business continuity capabilities.

Good business continuity plans will keep your company up and running through interruptions of any kind: power failures, IT system crashes, natural disasters, supply chain problems and more.

As a result, business continuity planning (BCP) is no longer a task executed only by wary IT leaders or cautious risk managers. Ensuring business continuity is the fiduciary and managerial responsibility of every corporate executive. Nor is business continuity a luxury, affordable only during economic good times. Like insurance, BCP is an expense that can protect against tremendous loss. It is a critical investment that, well-chosen, can deliver incomparable payoff.

Check Your Progress 1

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) Explain the main purpose of business continuity strategy.

.....

.....

.....

.....

2) What does continuity strategy include?

.....

.....

.....

.....

3) Which continuity strategies are commonly applied?

.....

.....

.....

.....

4) List the steps of developing a business continuity plan.

.....

.....

.....

.....

5) What are the main concerns of business continuity management strategies?

.....

.....

.....

.....

6) What services should be provided by a good business continuity solution?

.....

.....

.....

.....

4.8 LET US SUM UP

Many companies associate disaster recovery and business continuity only with IT and communications functions and miss other critical areas that can seriously impact their business. Other common areas for strategy development and selection are employees, facilities, power, customer service, billing, and customer and public relations. All areas require a clear well thought out strategy based on recovery time objectives cost and profitability impact. Strategy selection involves focusing on key risk areas and selecting a strategy for each one. The primary goals are to maintain business continuity in the face

of a disruption or disaster to recover, to key business functions quickly and to mitigate damages.

4.9 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

- 1) The purpose of the Business Continuity Strategy is to agree the priorities for recovery and to identify the resources that will be used to recover the business. Business Continuity strategy development should address:
 - The implementation of measures to increase the resilience of the organization to mitigate the impact of an incident
 - The use of alternative arrangements such as home or remote working or alternative office accommodation
 - The agreed recovery objectives that are achievable with the resources available
 - The responsibilities for Business Continuity and the structure of the response teams
 - The structure of the Business Continuity Plans
- 2) Continuity strategies may include:
 - action required to resume critical business activities
 - contact lists of critical personnel and stakeholders
 - counseling
 - critical business activities and prioritisation of when they can/need to resume
 - list of resources
- 3) Once your key activities and resources have been identified together with the associated risks, now it is important to decide that how you will manage these risks. The following lists of strategies are commonly applied:
 - Accept the risks and change nothing
 - Attempt to reduce the risks
 - Attempt to reduce the risks and make plans to restore key activities as soon as possible
 - Cease the activity altogether
- 4) The key steps in developing a business continuity plan are:

- Understanding your business
 - Business continuity management strategies
 - Developing and implementing a business continuity response
 - Developing a business continuity management culture
 - Exercising, maintenance and audit
- 5) Business Continuity Management Strategies concern:
- The selection of alternative operating methods to be used after an interruption to maintain or resume the organization's business activities and their dependencies (internal and external) to a priority, and time table determined in the Business Impact Analysis.
 - The protection of vulnerable and single points of failure in business critical processes identified in the Risk Analysis
- 6) Here are just some of the services that your business continuity solution should provide:
- Business Impact Analysis and Risk Analysis to protect the most profitable segments of your business
 - Resource Dependency Analysis to identify the processes and applications critical to the organization's business continuity.
 - Identifying and selecting appropriate and cost effective business continuity strategies,
 - Developing user friendly and maintainable business continuity plans.
 - Diverse options for testing continuity plans to confirm they are effective and build confidence in their use.

4.10 SUGGESTED READINGS

- http://securebusinesscontinuity.com/courses/Module_2_Business_Continuity_and_Disaster_Recovery.pdf
- <http://technet.microsoft.com/en-us/library/cc261687.aspx#DetermineStrategies>
- <http://www.activityim.com/services/business-continuity-planning/business-continuity-strategy/>
- <http://www.avalution.com/start/Pages/BusinessContinuityStrategyIdentification.aspx>

- <http://www.businesslink.gov.uk/bdotg/action/detail?itemId=1076147238&type=RESOURCES>
- <http://www.calamityprevention.com/training/Forbes-BCM-Good-Practice-Training-from-BCI.pdf>
- http://www.ehow.com/list_6365646_business-continuity-strategies.html#ixzz1UoZ15IPb
- <http://www.midwestdatarecovery.com/business-continuity-strategy.html>
- <http://www.parcor.com.au/images/stories/Microsoft%20Word%20%20BCM%20PDF%20for%20website.pdf>



Student Satisfaction Survey



Student Satisfaction Survey of IGNOU Students

Enrollment No.	
Mobile No.	
Name	
Programme of Study	
Year of Enrolment	
Age Group	☐ Below 30 ☐ 31-40 ☐ 41-50 ☐ 51 and above
Gender	☐ Male ☐ Female
Regional Centre	
States	
Study Center Code	

Please indicate how much you are satisfied or dissatisfied with the following statements

Sl. No.	Questions	Very Satisfied	Satisfied	Average	Dissatisfied	Very Dissatisfied
1.	Concepts are clearly explained in the printed learning material	☐	☐	☐	☐	☐
2.	The learning materials were received in time	☐	☐	☐	☐	☐
3.	Supplementary study materials (like video/audio) available	☐	☐	☐	☐	☐
4.	Academic counselors explain the concepts clearly	☐	☐	☐	☐	☐
5.	The counseling sessions were interactive	☐	☐	☐	☐	☐
6.	Changes in the counseling schedule were communicated to you on time	☐	☐	☐	☐	☐
7.	Examination procedures were clearly given to you	☐	☐	☐	☐	☐
8.	Personnel in the study centers are helpful	☐	☐	☐	☐	☐
9.	Academic counseling sessions are well organized	☐	☐	☐	☐	☐
10.	Studying the programme/course provide the knowledge of the subject	☐	☐	☐	☐	☐
11.	Assignments are returned in time	☐	☐	☐	☐	☐
12.	Feedbacks on the assignments helped in clarifying the concepts	☐	☐	☐	☐	☐
13.	Project proposals are clearly marked and discussed	☐	☐	☐	☐	☐
14.	Results and grade card of the examination were provided on time	☐	☐	☐	☐	☐
15.	Overall, I am satisfied with the programme	☐	☐	☐	☐	☐
16.	Guidance from the programme coordinator and teachers from the school	☐	☐	☐	☐	☐

After filling this questionnaire send it to:
 Programme Coordinator, School of Vocational Education and Training,
 Room no. 19, Block no. 1, IGNOU, Maidangarhi, New Delhi- 110068

NOTE

MPDD-IGNOU/P.O.1T/November, 2011

ISBN-978-81-266-5714-8