ignou
THE PEOPLE'S
UNIVERSITY

Indira Gandhi National Open University
School of Vocational Education and Training

MSEI-026
BCP, DR PLANNING AUDIT

DR Strategies

3

"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

Indira Gandhi National Open University
School of Vocational Education and Training

MSEI-026
BCP, DR Planning and Audit

Block

3

DR STRATEGIES

UNIT 1

Developing Plans for Computer System Recovery 5

UNIT 2

Developing Plans for Business Resumption 28

UNIT 3

Plan Templates and Software Tools 58

UNIT 4

Implementing Crisis Management Framework 85

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

ISBN: 978-81-266-7515-5

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 DR strategies. Computer Disaster Recovery is a methodology which encompasses the prospective plans to encounter an unfavorable condition in our computer repository where our important files are stored. We sometimes overlook this feature for software and database systems - until it is too late. Let us give a thought how our business would function if the computer systems and software vanished. This block comprises of four units and is designed in the following way;

The **Unit One** is an effort towards answering some of the fundamental queries about developing plans for computer system recovery. It provides a technical knowhow about Computer System Failures/Crashes and how to cope up with the same. It gives you a deep insight as to what Backup and Recovery measures are to be employed for avoidance of data loss.

The **Unit two** provides an overview of the developing plans for business resumption. A Business Resumption Plan (BRP) is a plan activated during or immediately after an emergency and is aimed at permitting the rapid and cost effective resumption of an organizations essential operations in order to maintain continuity of services to it's clients. It sets the stage for, but is a separate entity from, long term disaster recovery which returns the organization to normal operating conditions.

The **Unit three** covers plan templates and software tools. This unit is an effort towards the management of the project, i.e. planning and organizing resources to bring about the successful completion of specific goals while managing constraints of scope, costs and time. We have tried to give an overview of how to define a project, defining timeline, and managing.

The **Unit four** covers implementing crisis management framework. The field of crisis management is rising in scope and sophistication. Such changes should be acknowledged by recognizing that crisis management should be apart of the strategic management process. A crisis management framework should be designed that recognizes the various phases of the crisis management process. A framework is important because it guides us through the process of crisis management in a systematic manner that is both reactive and proactive.

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 DEVELOPING PLANS FOR COMPUTER SYSTEM RECOVERY

Structure

1.0 Introduction

1.1 Objectives

1.2 Understanding System Failures

- 1.2.1 Causes of System Failures/ Crashes
- 1.2.2 Back-ups and Recovery from Failure/Crashes
- 1.2.3 Storage Media for Back-ups and Recovery

1.3 Computer Disaster Recovery Plans

- 1.3.1 Computer Disaster Recovery Issues
- 1.3.2 Plan to Recover From the IT Disaster Scenarios

1.4 Backup and Recovery Technologies

- 1.4.1 Shadow Copies of Shared Folders overview
- 1.4.2 Windows Server Backup overview

1.5 Installation of Windows Server Backup Tools

1.6 How to Backup Documents in Windows XP- step by step guide

1.7 Let Us Sum Up

1.8 Check Your Progress: The key

1.9 Suggested Readings

1.0 INTRODUCTION

In today's scenario computers are used in each and every facet of our lives, be it education, be it entertainment, shopping or simple housekeeping tasks. Our life is dependent on the computer while we are at home, traveling, at the workplace etc. Computer has become an inseparable gadget in our life. But what if it stops working or behaves abnormally? Obviously it affects us too much personally as well as professionally. Have we ever thought of the potential causes that why our system crashes? Probably not only this, we got to analyze and formulate some concrete plans for cure of the problem.

In this chapter we would be basically discussing about system failure, recovery plans, recovering from this condition.

A **system crash** in computing is a condition where a computer or a program, either an application or part of the operating system ceases to function properly, often exiting after encountering errors. Often the offending program may appear to freeze or hang until a crash reporting service documents details of the crash. If the program is a critical part of the operating system kernel, the entire computer may crash. This is different from a hang or freeze where the application or OS continues to run without obvious response to input.

Many crashes are the result of the execution of a single machine instruction. The characteristic causes are when the program counter is set to an incorrect address or a buffer overflow overwrites a portion of program code due to an earlier bug. In either case, it is quite common for the processor to attempt to execute data or random memory values. Since all data values are possible but only some values are valid instructions, this often results in an illegal instruction exception.

DR strategies are framed so as to encounter these undesirable conditions as system failure or crash. Some back-up software and recovery tools are used for the purpose.

These have to be pre-planned before we actually get stricken in this kind of situation so that the loss of data and recovery time are minimized.

1.1 OBJECTIVES

After studying this unit, you should be able to:

- identify potential causes of system crashes;
- understand the risks of system crash;
- need of backup and recovery methodologies;
- explain the disaster recovery planning; and
- types of backup mechanisms.

1.2 UNDERSTANDING SYSTEM FAILURES

The term "System Failure" or "Computer System crash" refers to a critical failure in a computer, network device, or software running on these (such as a network operating system or application). Crashes often occur with little or no warning.

1.2.1 Causes of System Failures / Crashes

a) Hardware Conflict

The one prominent reason why Windows crashes is hardware conflict. Each hardware device communicates to other devices through an interrupt request channel (IRQ) which must be unique for each device.

For example, a printer usually connects internally on IRQ 7. The keyboard usually uses IRQ 1 and the floppy disk drive IRQ 6. Each device will try to hog a single IRQ for itself.

If there are a lot of devices, or if installation of these devices is not done properly, those may end up sharing the same IRQ number. When the user tries to use both devices at the same time, it will result in a clash. The way to check if your computer has a hardware conflict is through the following route:

Start-Settings-Control Panel-System-Device Manager

Often if a device has a problem a yellow '!' appears next to its description in the Device Manager. Highlight Computer (in the Device Manager) and press Properties to see the IRQ numbers used by your computer. If the IRQ number appears twice, two devices may be using it.

Sometimes a device might share an IRQ with something described as 'IRQ holder for PCI steering'. This can be ignored. The best way to fix this problem is to remove the problem device and reinstall it.

b) Bad RAM

RAM (random-access memory) problems might bring on the blue screen of death with a message saying Fatal Exception Error. A fatal error indicates a serious hardware problem. Sometimes it may mean a part is damaged and will need replacing.

A fatal error caused by RAM might be due to a mismatch of chips. For example, mixing 70-nanosecond (70ns) RAM with 60ns RAM will usually force the computer to run the entire RAM at the slower speed. This will often crash the machine if the RAM is overworked.

One way around this problem is to enter the BIOS settings and increase the wait state of the RAM. This can make it more stable. Another way to troubleshoot a suspected RAM problem is to rearrange the RAM chips on the motherboard, or take some of them out. Then try to repeat the circumstances that caused the crash.

c) Hard Disk Drives

The information on a hard disk drive starts getting fragmented after sometime so it is good to defragment the hard disk at frequent intervals, to prevent the disk from causing a screen freeze. Go to

Start → Programs →Accessories → System → Tools → Disk Defragmenter

Consequently a procedure will be started. You will be unable to write data to the hard drive (to save it) while the disk is defragmenting, so it is a good idea to schedule the procedure for a period of inactivity using the Task Scheduler.

Some lockups and screen freezes caused by hard disk problems can be solved by reducing the read-ahead optimisation. This can be adjusted by going to:

Start→ Settings→ Control Panel→ System Icon→ Performance→ File System→ Hard Disk

Hard disks will slow down and crash if they are too full. So some housekeeping is needed to be done on the hard drive every few months and free some space on it. Open the Windows folder on the C drive and find the Temporary Internet Files folder. Deleting the contents (not the folder) can free a lot of space.

Empty the Recycle Bin every week to free more space. Hard disk drives should be scanned every week for errors or bad sectors. Go to

Start→Program →Accessories →System →Tools →ScanDisk

Otherwise assign the Task Scheduler to perform this operation at night when the computer is not in use.

d) Fatal OE Exceptions and VXD Errors

Fatal OE exception errors and VXD errors are often caused by video card problems.

These can often be resolved easily by reducing the resolution of the video display. Go to

Start→ Settings→ Control Panel→ Display→ Settings

Here you should slide the screen area bar to the left. Take a look at the colour settings on the left of that window. For most desktops, high colour 16-bit depth is adequate.

If the screen freezes or you experience system lockups it might be due to the video card. Make sure it does not have a hardware conflict. Go to

Start→ Settings→ Control Panel→ System→ Device Manager

Select the + beside Display Adapter. A line of text describing your video card should appear. Select it (make it blue) and press properties. Then select Resources and select each line in the window. Look for a message that says No Conflicts.

If you have video card hardware conflict, you will see it here. Be careful at this point and make a note of everything you do in case you make things worse.

The way to resolve a hardware conflict is to uncheck the Use Automatic Settings box and hit the Change Settings button. You are searching for a setting that will display a No Conflicts message.

Another useful way to resolve video problems is to go to

Start→ Settings→ Control Panel→ System→ Performance→ Graphics

Here you should move the Hardware Acceleration slider to the left. As ever, the most common cause of problems relating to graphics cards is old or faulty drivers (a driver is a small piece of software used by a computer to communicate with a device).

e) Viruses

Often the first sign of a virus infection is instability. Some viruses erase the boot sector of a hard drive, making it impossible to start. This is why it is a good idea to create a Windows start-up disk. Go to

Start→ Settings→ Control Panel→ Add/Remove Programs

Here, look for the Start Up Disk tab. Virus protection requires constant vigilance.

A virus scanner requires a list of virus signatures in order to be able to identify viruses. These signatures are stored in a DAT file.

f) Printers

The action of sending a document to print creates a bigger file, often called a postscript file.

Printers have only a small amount of memory, called a buffer. This can be easily overloaded. Printing a document also uses a considerable amount of CPU power. This will also slow down the computer's performance.

If the printer is trying to print unusual characters, these might not be recognized, and can crash the computer. Sometimes printers will not recover from a crash because of confusion in the buffer. A good way to clear the buffer is to unplug the printer for ten seconds. Booting up from a powerless state, also called a cold boot, will restore the printer's default settings and you may be able to carry on.

g) Software

A common cause of computer crash is faulty or badly-installed software. Often the problem can be cured by uninstalling the software and then reinstalling it. This will also remove references to the programme in the System Registry and leaves the way clear for a completely fresh copy.

The System Registry can be corrupted by old references to obsolete software that you thought was uninstalled. Read the instructions and use it carefully so you don't do permanent damage to the Registry. If the Registry is damaged you will have to reinstall your operating system. Often a Windows problem can be resolved by entering Safe Mode. This can be done during start-up. When you see the message "Starting Windows" press F4. This should take you into Safe Mode.

Safe Mode loads a minimum of drivers. It allows you to find and fix problems that prevent Windows from loading properly.

Sometimes installing Windows is difficult because of unsuitable BIOS settings. If you keep getting SUWIN error messages (Windows setup) during the Windows installation, then try entering the BIOS and disabling the CPU internal cache. Try to disable the Level 2 (L2) cache if that doesn't work.

Remember to restore all the BIOS settings back to their former settings following installation.

h) Overheating

Central processing units (CPUs) are usually equipped with fans to keep them cool. If the fan fails or if the CPU gets old it may start to overheat and generate a particular kind of error called a kernel error. This is a common problem in chips that have been overclocked to operate at higher speeds than they are supposed to.

One remedy is to get a bigger better fan and install it on top of the CPU. CPU problems can often be fixed by disabling the CPU internal cache in the BIOS. This will make the machine run more slowly, but it should also be more stable.

i) Power Supply Problems

A power surge can crash a computer as easily as a power cut.

If this has become a nuisance for you then Uninterrupted Power Supply (UPS) should be connected to the system. This will give you a clean power supply when there is no electricity, and it will give you a few minutes to perform a controlled shutdown in case of a power cut.

1.2.2 Back-ups and Recovery from Failure/Crashes

Backup or the process of **backing up** refers to making copies of data so that these additional copies may be used to *restore* the original after an event of data loss.

What is the purpose of Backup?

The foremost purpose is to recover data in response to data loss, be it by data deletion or corrupted data. Data loss is a very common experience of computer users.

The secondary purpose of backups is to recover data from a historical period of time within the constraints of a user-defined data retention policy, typically configured within a backup application for how long copies of data are required.

Since a backup system contains at least one copy of all data worth saving, the data storage requirements are considerable. Organizing this storage space and managing the backup process is a complicated undertaking. A Data Repository Model may be used to provide configuration to the storage. In the modern era of computing there are many different types of data storage devices that are useful for making backups. There are also many different ways in which these devices can be arranged to provide data security, and portability.

Before data is sent to its storage location, it goes through a chain of procedures as it is selected, extracted, and manipulated. Many different methods have been designed to optimize the backup procedure. These include optimizations for dealing with open files and live data sources as well as compression, encryption, and duplication, among others. Many organizations and individuals try to have confidence that the process is working as expected and work to define measurements and validation techniques. It is also important to recognize the limitations and human factors involved in any backup scheme.

1.2.3 Storage Media for Back-ups and Recovery

Regardless of the repository model that is used, the data has to be stored on some data storage medium somewhere.

a) Magnetic tape

Magnetic tape has long been the most commonly used medium for bulk data storage, backup, archiving, and interchange. Tape has typically had an order of magnitude better capacity/price ratio when compared to hard disk, but recently the ratios for tape and hard disk have become a lot closer. There are myriad formats, many of which are proprietary or specific to certain markets like mainframes or a particular brand of personal computer. Tape is a sequential access medium, so even though access times may be poor, the rate of continuously writing or reading data can actually be very fast. Some new tape drives are even faster than modern hard disks. A principal advantage of tape is that it has been used for this purpose for decades (much longer than any alternative) and its characteristics are well understood.

Hard Disk

The capacity/price ratio of hard disk has been rapidly improving for many years. This is making it more competitive with magnetic tape as a bulk storage medium. The main advantages of hard disk storage are low access times, availability, capacity and ease of use. External disks can be connected via local interfaces like SCSI, USB, FireWire, or eSATA, or via longer distance technologies like Ethernet, iSCSI, or Fibre Channel. Some disk-based backup systems, such as Virtual Tape Libraries, support data deduplication which can dramatically reduce the amount of disk storage capacity consumed by daily and weekly backup data. The main disadvantages of hard disk backups are that they are easily damaged, especially while being transported (e.g., for off-site backups), and that their stability over periods of years is a relative unknown.

b) Optical Storage

Recordable Cds and DVDs, and Blu-ray Discs are commonly used with personal computers and generally have low media unit costs. However, the capacities and speeds of these and other optical discs are typically an order of magnitude lower than hard disk or tape. Many optical disk formats are WORM type, which makes them useful for archival purposes since the data can't be changed. The use of an auto-changer or jukebox can make optical discs a feasible option for larger-scale backup systems. Some optical storage systems allow for cataloged data backups without human contact with the discs, allowing for longer data integrity.

c) Floppy Disk

During the 1980s and early 1990s, many personal/home computer users associated backing up mostly with copying to floppy disks. The low data capacity of a floppy disk makes it an unpopular and obsolete choice today.

d) Solid State Storage

Also known as flash memory, thumb drives, USB flash drives, CompactFlash, SmartMedia, Memory Stick, Secure Digital cards, etc., these devices are relatively costly for their low capacity, but offer excellent portability and ease-of-use.

e) **Remote Backup Service**

In today's scenario the broadband internet access becomes more pervasive, remote backup services are gaining in popularity. Backing up via the internet to a remote location can protect against some worst-case situation such as fires, floods, or earthquakes which would destroy any backups in the immediate vicinity along with everything else. There are, however, a number of drawbacks to remote backup services. First, Internet connections are usually slower than local data storage devices. Residential broadband is especially problematic as routine backups must use an upstream link that's usually much slower than the downstream link used only occasionally to retrieve a file from backup. This tends to limit the use of such services to relatively small amounts of high value data. Secondly, users must trust a third party service provider to maintain the privacy and integrity of their data, although confidentiality can be assured by encrypting the data before transmission to the backup service with an encryption key known only to the user. Ultimately the backup service must itself use one of the above methods so this could be seen as a more complex way of doing traditional backups.

1.3 COMPUTER DISASTER RECOVERY PLANS

Computer Disaster Recovery is a methodology which encompasses the prospective plans to encounter an unfavorable condition in our computer repository where our important files are stored. We sometimes overlook this feature for software and database systems - until it is too late. Let us give a thought how our business would function if the computer systems and software vanished. Here are some questions to think about when planning for next flood, hurricane, tornado or other catastrophe - large or small.

1.3.1 Computer Disaster Recovery Issues

a. Is the backup of the software and databases taken on a regular basis?

b. Is the database or spreadsheet copied to the same place every time, over writing the previous one?

c. Is the copy kept offsite?

d. How can the database or software be accessed without going to the workplace?

e. Is the backup of the software stored on a server which in turn is backed up by the computer department?

f. How long it will take the Information Technology department to retrieve a server backup? In many cases it will takes days and in some cases weeks.

g. Is the data backup tested properly to make sure it is a good copy of the software and not corrupted?

h. Are the critical program passwords stored in a secure place known by officers of a company so that they can get to the program in the event that developer/designer is permanently unavailable?

1.3.2 Plan to Recover From the IT Disaster Scenarios

First part of database disaster recovery is easy - backup database systems on a regular basis.

Maintain a minimum of 3 consecutive copies before overwriting.

Consider doing a backup each day of the week:

1) Take a copy home

2) Send to a website located in another city/state

3) Regular courier to another corporate office

4) Establish an offsite backup service with courier pickup (for more critical databases)

- Retain Friday's backup for at least six months
- Every six month retain the most recent backup for permanent offsite storage
- Get the database into your corporate data backup system if this is available.
- Save key passwords and a copy of documentation in a secure place known by corporate officers
- Periodically test the backups and the disaster recovery procedure to assure that you can get the software up and running again in a timely fashion.

For larger more critical databases consider the following in your corporate disaster recovery planning.

Database Disaster Recovery Planning Checklist for Critical Systems

- Develop a written business continuity plan.
- Identify roles and responsibilities.

- Identify backup personnel for each role.
- Identify a backup location for the use of your database.
- Consider having reciprocal office sharing agreements with a company in the next town.
- Identify necessary computer hardware configuration and software in case it needs to be replaced. For larger companies have POs already written and ready to go.
- Do a walkthrough of your disaster recovery plan.
- Practice a real activation of your DRP annually.
- Store the plan and all necessary documentation offsite.
- Consider hiring a disaster recovery planning consultant
- Practice Safe Computing

A good anti-virus program can save you a lot of grief. Running an anti-virus program daily and a spyware blocker once every week or two will protect you from most threats and annoyances. Internet cookies accumulate as you surf, and can build up to the point where your machine slows down. Links to good free anti-virus and anti-software programs, and cookie cleaning programs, are found in Resources. The cookie program Cleaner also includes a fully featured registry cleaner.

A word of caution regarding e-mail: Never click on a link in e-mail, unless you know the sender and were expecting to be sent a link. Read all e-mails that purport to come from your bank or any financial institution very carefully. E-mails originating from a financial institution always address you by name, never ask for your password, and never ask you to click on a link. Identity theft is even worse than a computer meltdown.

1.4 BACKUP AND RECOVERY TECHNOLOGIES

There are several features in Windows Server 2008 that you can use together to create backups and perform recoveries of your server systems and data. These include the following:

- **Shadow Copies of Shared Folders**
- **Windows Server Backup tools** (including the Windows Server Backup Microsoft Management Console (MMC) snap-in, the **Wbadmin** command-line tool, and the Windows PowerShell commands for Windows Server Backup)

- **Windows Recovery Environment** (including Windows Complete PC Restore, Windows Memory Diagnostic Tool, and Command Prompt)

You can use these tools to perform the following backup or recovery tasks for your computers running Windows Server 2008:

1.4.1 Shadow Copies of Shared Folders Overview

Shadow Copies of Shared Folders provides point-in-time copies of files that are located on shared resources, such as a file server.

What is Shadow Copies of Shared Folders?

Shadow Copies of Shared Folders is a feature included in the Shared Folders Microsoft Management Console (MMC) snap-in that you or your users can use to view shared files and folders as they existed at points of time in the past. Accessing previous versions of files, or shadow copies, is useful because you can:

- **Recover files that were accidentally deleted.** If you accidentally delete a file, you can open a previous version and copy it to a safe location.
- **Recover from accidentally overwriting a file.** If you accidentally overwrite a file, you can recover a previous version of the file.
- **Compare versions of a file while working.** You can use previous versions when you want to check what has changed between two versions of a file.

However, creating shadow copies is not a replacement for creating regular backups. Also, you can only enable Shadow Copies of Shared Folders on a per-volume basis—that is, you cannot select specific shared folders and files on a volume to be copied or not copied.

Hardware and software considerations for Shadow Copies of Shared Folders

Shadow Copies of Shared Folders is available in all editions of Windows Server 2008 (both 32-bit and 64-bit versions). However, the Shadow Copies of Shared Folders user interface is not available for the Server Core installation option of Windows Server 2008.

- If you plan to defragment the source volume on which Shadow Copies of Shared Folders is enabled, it is recommended that you set the cluster allocation unit size to be 16 KB or larger when you initially format the source volume. If you do not, the number of changes caused by defragmentation can cause previous versions of files to be deleted.

1.4.2 Windows Server Backup Overview

Windows Server Backup is a feature in Windows Server 2008 that provides a set of wizards and other tools for you to perform basic backup and recovery tasks for your servers running Windows Server 2008. This feature has been redesigned and introduces new technology. The previous backup feature (Ntbackup.exe) that was available with earlier versions of Windows has been removed.

What is Windows Server Backup?

The Windows Server Backup feature in Windows Server 2008 consists of an MMC(Microsoft management Control) snap-in and command-line tools that provide a complete solution for your day-to-day backup and recovery needs. There are four wizards to guide through running backups and recoveries. Windows Server Backup is used to backup a full server (all volumes), selected volumes, or the system state. The volumes, folders, files, certain applications, and the system state can easily be recovered. And, in case of disasters like hard disk failures, a system recovery can be performed by using a full server backup and the Windows Recovery Environment—this will restore the complete system onto the new hard disk.

Windows Server Backup is used to create and manage backups for the local computer or a remote computer. Also, backups may be scheduled to run automatically.

Windows Server Backup is intended for use by everyone who needs a basic backup solution—from small business owners to IT professionals in large enterprises. However, the design makes it especially well-suited for smaller organizations or individuals who are not IT professionals.

Windows Recovery Environment overview

Windows Recovery Environment in Windows Server 2008 is a partial version of the operating system and a set of tools that you can use to perform operating system or full server recoveries (along with a backup that you created earlier using Windows Server Backup).

Features in Windows Recovery Environment

The tools in Windows Recovery Environment include:

- **Windows Complete PC Restore**. This tool is basically used and a backup that you created earlier with Windows Server Backup to restore your operating system or full server.
- **Windows Memory Diagnostic Tool**. This tool (which is a memory diagnostic schedule) is used to check your computer's RAM. Doing this

requires a restart. In addition, this tool requires a valid Windows Server 2008 (or Windows Vista) installation to function.

- **Command Prompt**. This opens a command prompt window with Administrator privileges that provides full access to your file system and volumes. In addition, certain **Wbadmin** commands are only available from this command window.

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 meant by System Crash?

....

....

....

....

2) List any five potential causes for System Failure.

....

....

....

....

3) What do understand by Storage Media? Explain any one.

....

....

....

....

4) State the Computer Disaster Recovery Issues?

....

....

....

....

1.5 INSTALLATION OF WINDOWS SERVER BACKUP TOOLS

To access backup and recovery tools, you must install the **Windows Server Backup Features** and subordinate items that are available in the Add Features Wizard in Server Manager. This installs the following tools:

- Windows Server Backup Microsoft Management Console (MMC) snap-in
- **Wbadmin** command-line tool
- Windows PowerShell cmdlets for Windows Server Backup
- To install Backup and Recovery Tools:

To install Backup and Recovery Tools:

1. Click **Start**, click **Server Manager**, in the left pane click **Features**, and then in the right pane click **Add Features**. This opens the Add Features Wizard.
2. In the Add Features Wizard, on the **Select Features** page, expand **Windows Server Backup Features**, and then select the check boxes for **Windows Server Backup** and **Command-line Tools**.

   You will receive a message that Windows PowerShell is also required to be installed with these features.
3. Click **Add Required Features**, and then click **Next**.
4. On the **Confirm Installation Selections** page, review the choices that you made, and then click **Install**. If there is an error during the installation, it will be noted on the **Installation Results** page.
5. Then, to access these backup and recovery tools, do the following:
   1. To access the Windows Server Backup snap-in, click **Start**, click **Administrative Tools**, and then click **Windows Server Backup**.
   2. To access and view the syntax for **Wbadmin**, click **Start**, right-click **Command Prompt**, and then click **Run as administrator**. At the prompt, type: **wbadmin /?**

1.6 HOW TO BACKUP DOCUMENTS IN WINDOWS XP-STEP BY STEP GUIDE

Step 1 First, load the backup software. You can find it by clicking

Start→ Accessories→ System Tools→ Backup

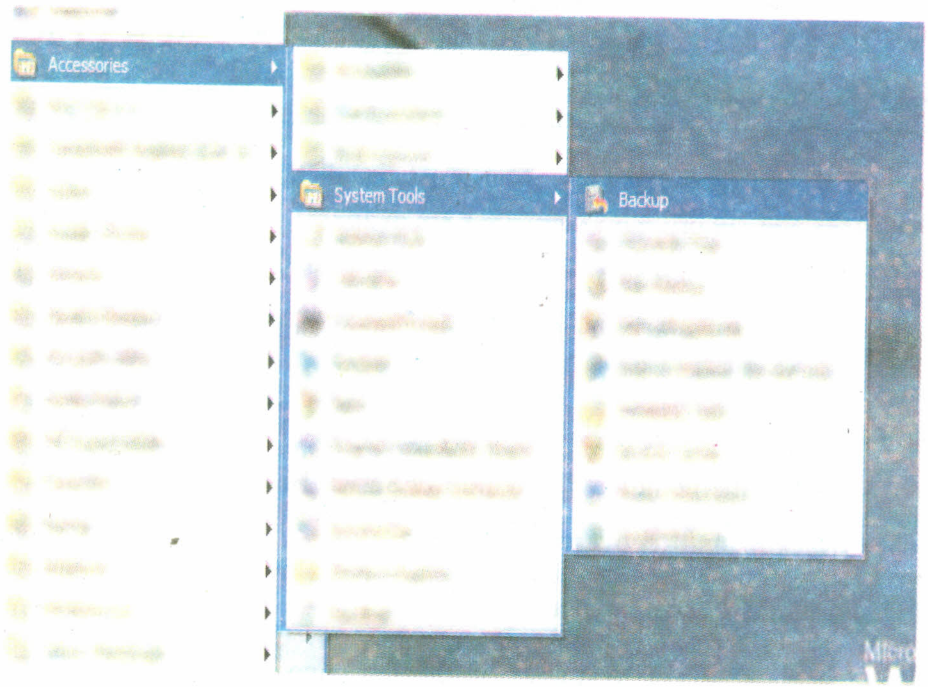


Fig. 1

Step 2 Wait for the application to load. (If the screen doesn't look like the picture below, click switch to Wizard Mode.) Then click Next.

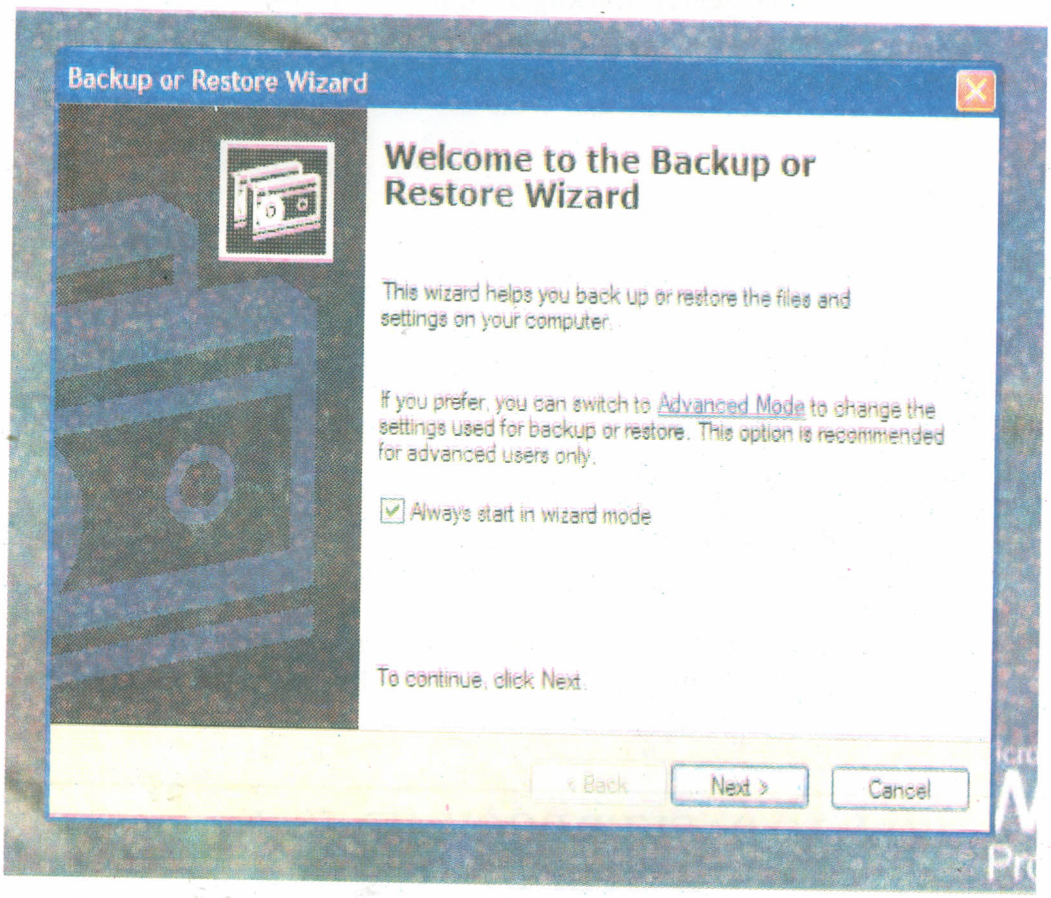


Fig. 2

Step 3 On the next screen, the wizard will ask you what you want to do. Select 'Back up files and settings' and click Next.

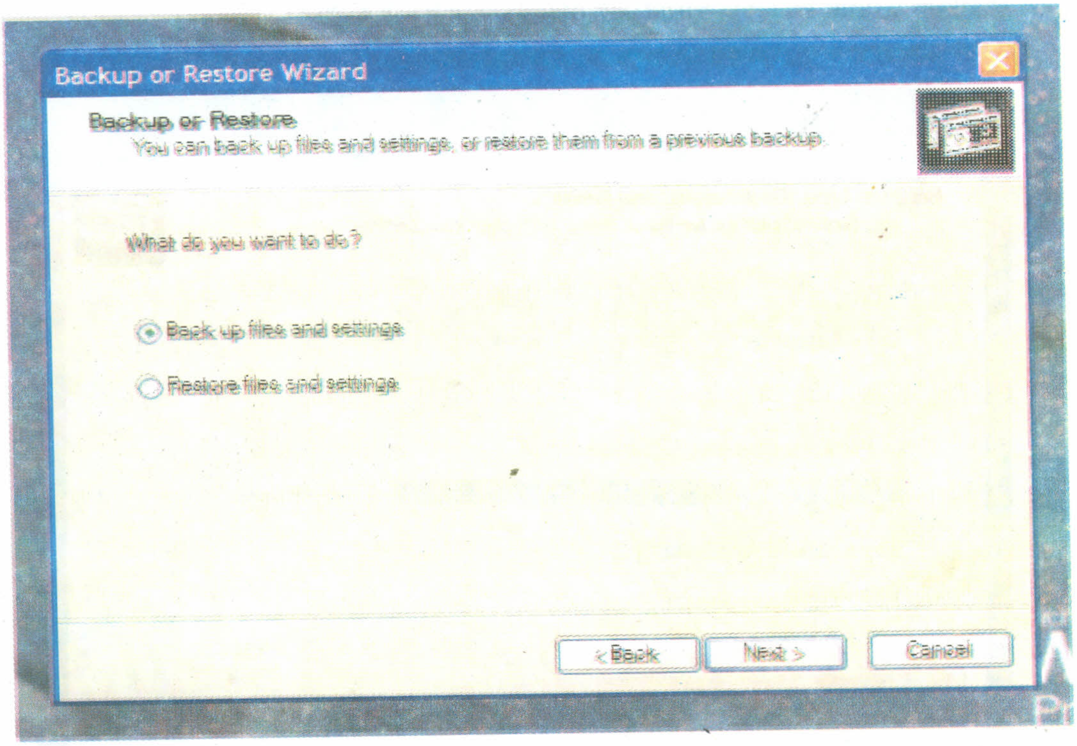


Fig. 3

Step 4 At this step, the wizard will ask you what you want to back up. The options are self explanatory – most importantly you'll want to either backup your documents and settings, or everyone's documents and settings. Select an option, and click Next.

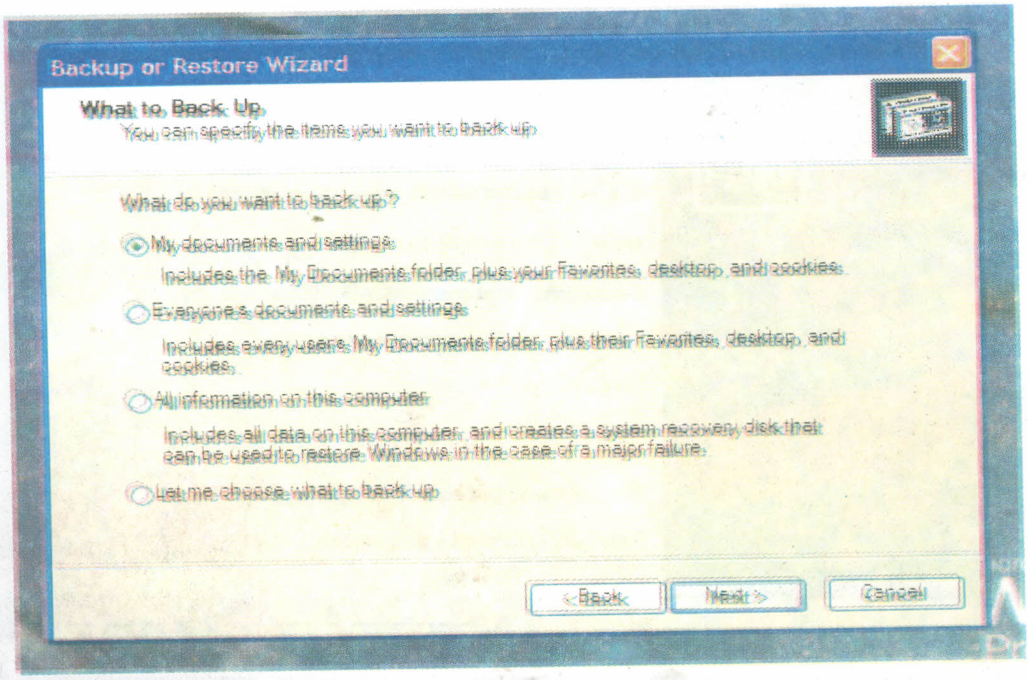


Fig. 4

Step 5 Choose where to save your back up. Choose the corresponding letter from the middle drop down (labelled F: in the picture). Name the back up (Data Backup would be an appropriate name). Then click Next.

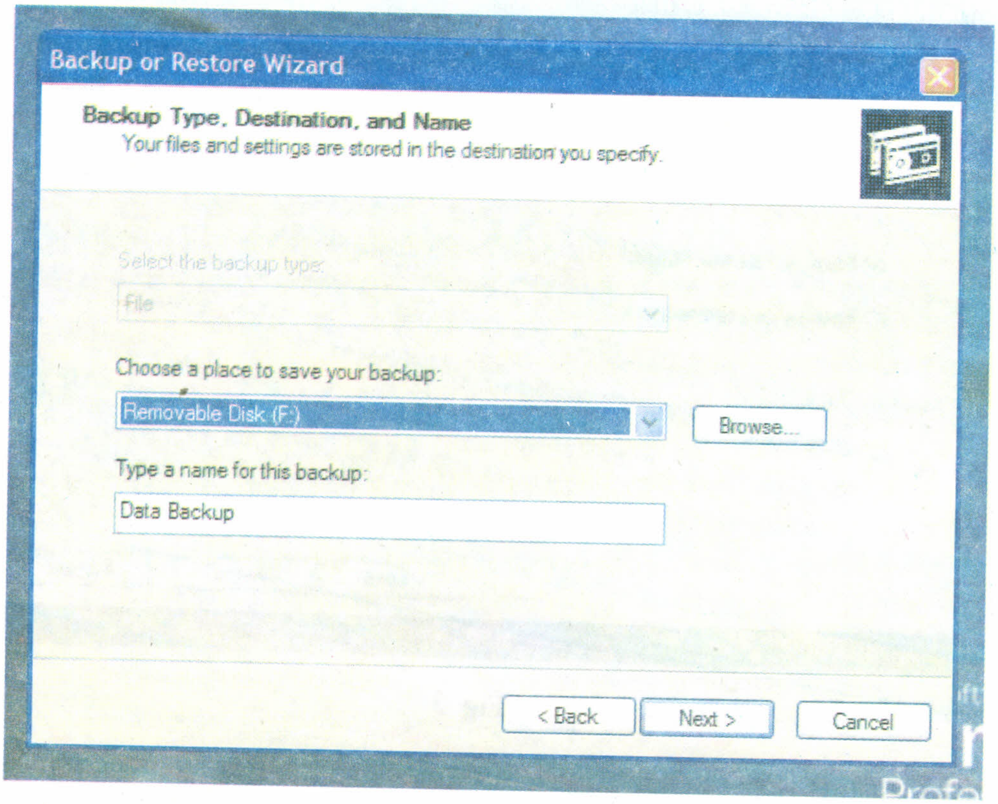


Fig. 5

Step 6 Review the settings, and click Finish.

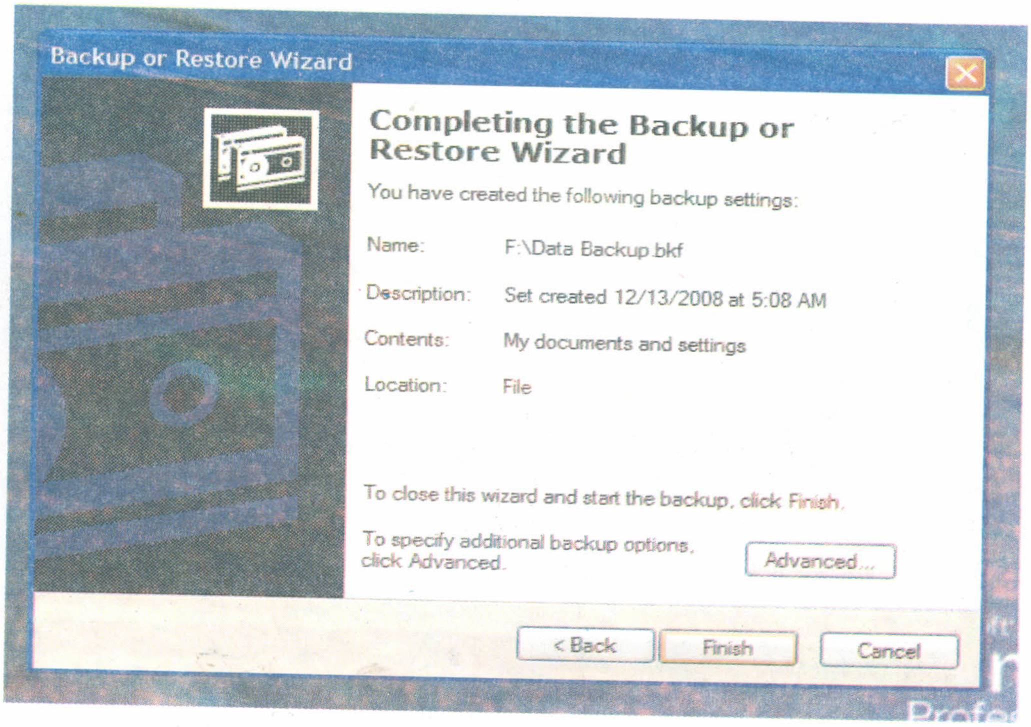


Fig. 6

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 meant by Window Server Backup?

....

....

....

....

2) Explain the tools of window recovery environment.

....

....

....

....

3) List all the options which are provided for step "What do you want to backup?" in Backup and Recovery Wizard.

....

....

....

....

4) How is Window server 2008 recovered?

....

....

....

....

1.7 LET US SUM UP

This unit provides you a technical know how about Computer System Failures/Crashes and how to cope up with the same. It gives you a deep insight as to what Backup and Recovery measures are to be employed for avoidance of data loss.

It lets us know the Disaster Recovery Strategies and issues to be aware of, for practicing safe computing.

This unit has been designed to make the pupils informed about the hazards of data loss and tricks to cope up with the computer disaster through Easy Recovery Processes.

This unit also deals with the Window XP Documents which is a step by step guide to enable the students to have hands-on experience of the same.

Since all the work in every facet of life is automated nowadays so the information security is an issue to be pondered upon very deeply and efficiently because our information is vulnerable to the damages, intentional and unintentional losses and tampering.

1.8 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

1) A **system crash** in computing is a condition where a computer or a program, either an application or part of the operating system ceases to function properly, often exiting after encountering errors. Often the offending program may appear to freeze or hang until a crash reporting service documents details of the crash. If the program is a critical part of the operating system kernel, the entire computer may crash. This is different from a hang or freeze where the application or OS continues to run without obvious response to input.

2) The causes of System Failure are :

   a Hardware Conflict

   b Viruses

   c Bad RAM

   d Fatal Errors in Graphics card.

3) The storage media are the devices where the data can be stored like hard disks, magnetic tapes, magnetic disks, CDs and DVDs and Flash Drives etc. These prove to be a very good and efficient sources of data storage for the purpose of backup.

   Optical Storage: Recordable CDs and DVDs, and Blu-ray Discs are commonly used with personal computers and generally have low media unit costs. However, the capacities and speeds of these and other optical discs are typically an order of magnitude lower than hard disk or tape. Many optical disk formats are WORM type, which makes them useful for archival purposes since the data can't be changed. The use of an auto-changer or jukebox can make optical discs a feasible option for larger-scale backup systems. Some optical storage systems allow for cataloged data backups without human contact with the discs, allowing for longer data integrity.

4) The disaster recovery issues are as follows:

- Is the backup of the software and databases taken on a regular basis?
- Is the database or spreadsheet copied to the same place every time, over writing the previous one?
- How long it will take the Information Technology department to retrieve a server backup? In many cases it will takes days and in some cases weeks.
- Is the data backup tested properly to make sure it is a good copy of the software and not corrupted?
- Are the critical program passwords stored in a secure place known by officers of a company so that they can get to the program in the event that developer/designer is permanently unavailable?
- Is the copy kept offsite?
- How can the database or software be accessed without going to the workplace?
- Is the backup of the software stored on a server which in turn is backed up by the computer department?

Check Your Progress 2

1) The Windows Server Backup feature in Windows Server 2008 consists of an MMC(Microsoft management Control) snap-in and command-line tools that provide a complete solution for your day-to-day backup and recovery needs. There are four wizards to guide through running backups and recoveries. Windows Server Backup is used to backup a full server (all volumes), selected volumes, or the system state. The volumes, folders, files, certain applications, and the system state can easily be recovered. And, in case of disasters like hard disk failures, a system recovery can be performed by using a full server backup and the Windows Recovery Environment—this will restore the complete system onto the new hard disk.

2) **The tools in Windows Recovery Environment include:**

- **Windows Complete PC Restore**. This tool is basically used and a backup that is created earlier with Windows Server Backup to restore the operating system or full server.

- **Windows Memory Diagnostic Tool**. This tool (which is a memory diagnostic schedule) is used to check your computer's RAM. Doing this requires a restart. In addition, this tool requires a valid Windows Server 2008 (or Windows Vista) installation to function.

- **Command Prompt**. This opens a command prompt window with Administrator privileges that provides full access to your file system and volumes. In addition, certain **Wbadmin** commands are only available from this command window.

3) "What do you want to back up?" in the Backup or Restore Wizard gives four options:

   a My documents and settings

   b Everyone's documents and settings

   c All information on this system

   d Let me choose what to back up

4) Install the **Windows Server Backup Features** and subordinate items that are available in the Add Features Wizard in Server Manager. This installs the following tools:

   - Windows Server Backup Microsoft Management Console (MMC) snap-in

   - **Wbadmin** command-line tool

   - Windows PowerShell cmdlets for Windows Server Backup

To Install Backup and Recovery Tools:

- Click **Start**, click **Server Manager**,
  - in the left pane clicks **Features**,
  - in the right pane click **Add Features which will** open the **Add Features Wizard**.
- In the Add Features Wizard, on the **Select Features** page
  - expand **Windows Server Backup Features**
  - select the check boxes for **Windows Server Backup** and **Command-line Tools**.
  - a message reading Windows PowerShell is also required to be installed with these features is shown.
- Click **Add Required Features**, and then click **Next**.

- On the **Confirm Installation Selections** page, review the choices that you made, and then click **Install**. If there is an error during the installation, it will be noted on the **Installation Results** page.

- Then, to access these backup and recovery tools, do the following:

  - To access the Windows Server Backup snap-in, click **Start**, click **Administrative Tools**, and then click **Windows Server Backup**.

  - To access and view the syntax for **Wbadmin**, click **Start**

  - Right-click **Command Prompt**

  - Click **Run as administrator**.

  - At the prompt, type: wbadmin?

1.8 SUGGESTED READINGS

- http://technet.microsoft.com/en-us/library/cc7

- http://www.ideologics.co.uk

- Jeffrey R. Shapiro, "Windows Server 2008 Bible", Wiley Publishing Inc., 2008.

UNIT 2 DEVELOPING PLANS FOR BUSINESS RESUMPTION

Structure

2.0 Introduction
2.1 Objectives
2.2 Need of BRP
2.3 Goal of BRP
2.4 Business Resumption Planning
    2.4.1 Checklist
    2.4.2 BRP Format
2.5 BRP Phases
    2.5.1 Response Phase
    2.5.2 Resumption Phase
    2.5.3 Recovery Phase
    2.5.4 Restoration Phase
2.6 BRP Process
    2.6.1 Find out Critical Activities
    2.6.2 Find out Threats
    2.6.3 Approval through Management
    2.6.4 Develop a BRP Plan for the Organization
    2.6.5 Communicate BRP Plan to the Employee
    2.6.6 Test the BRP Plan
2.7 Review the BRP Plan
    2.7.1 Organizational Outputs
    2.7.2 Department Level Functions
    2.7.3 Determine Resource Needs
2.8 Let Us Sum Up
2.9 Check Your progress: The Key
2.10 Suggested Readings

2.0 INTRODUCTION

Business Resumption Plan (BRP) is a plan activated during or immediately after an emergency and is aimed at permitting the rapid and cost effective resumption of an organization's essential operations in order to maintain continuity of service to its clients.

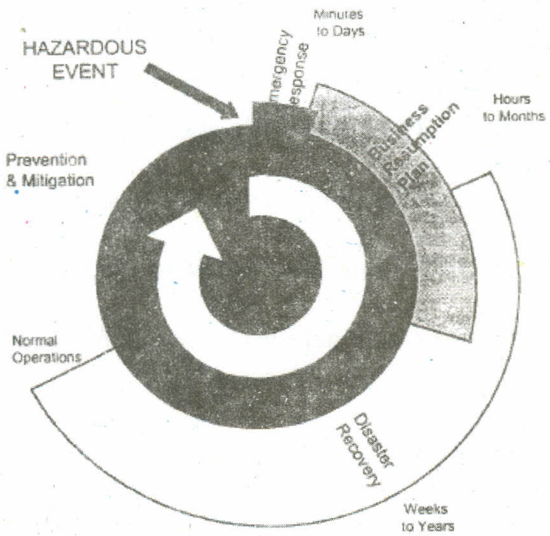


Fig. 1

The key elements include the following: The BRP has a defined response structure, and outlines individual responsibilities as well as providing action guidelines and the information necessary to carry out these activities time frame.

A BRP should not be confused with disaster recovery which implies a return to normal operations. The BRP is a temporary stage during which specific activities are undertaken to allow the organization to remain viable to its clients.

The BRP enables long term disaster recovery to take place eventually returning the organization to normal operating conditions that existed prior to the disaster. Recovery and Resumption Planning relates to recovering or resuming business and IT operations following incidents and disasters, typically from alternative locations, using fallback equipment etc.

Business Resumption Planning helps an organization to meet the growing demand of businesses and to develop comprehensive package of basic information necessary to assist organizations in developing and supporting a BRP.

2.1 OBJECTIVES

After studying this unit, you should be able to:

- understand the business resumption planning and its requirement in business;

- difference between business resumption planning and hazard management strategies;
- benefits of planning BRP and how it's able to recover the problem;
- understanding of the different phases of business resumption planning;
- how to develop the BRP planning specific to the business;
- prioritize the functions and activities on the basis of criticality of the activity;
- in a disaster scenario, how to initiate the BRP plan;
- creating different team and leaders and integrate them; and
- how the information is smoothly and timely moves to handle and recover the situation.

2.2 NEED OF BRP

In the scenario of 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.

In the event of a disaster or other circumstances, the normal operations of the organization may stuck and will shift the organization into contingency organization The major areas that may effect in case of such circumstances are-

Productivity

- Loss Of Productivity
- Employees Impacted @ X Burdened Hourly Rate

Legal/Regulatory

- Contractual Requirements
- SLAs
- Regulatory Requirements

Revenue

- Direct Loss
- Deferred Losses
- Compensatory Payments
- Lost Future Revenue
- Billing Losses
- Investment Losses

Financial Performance

- Lost Market Share
- Revenue Recognition
- Cash Flow
- Lost Discounts
- Payment Guarantees
- Stock Price
- Credit Rating

Other Expenses

- Temporary employees,
- Equipment Rental,
- Overtime,
- Extra Shipping Costs,
- Travel Expenses,
- Etc.

Reputation

- Customers
- Suppliers
- Financial Markets
- Banks

- Business Partners
- Etc.

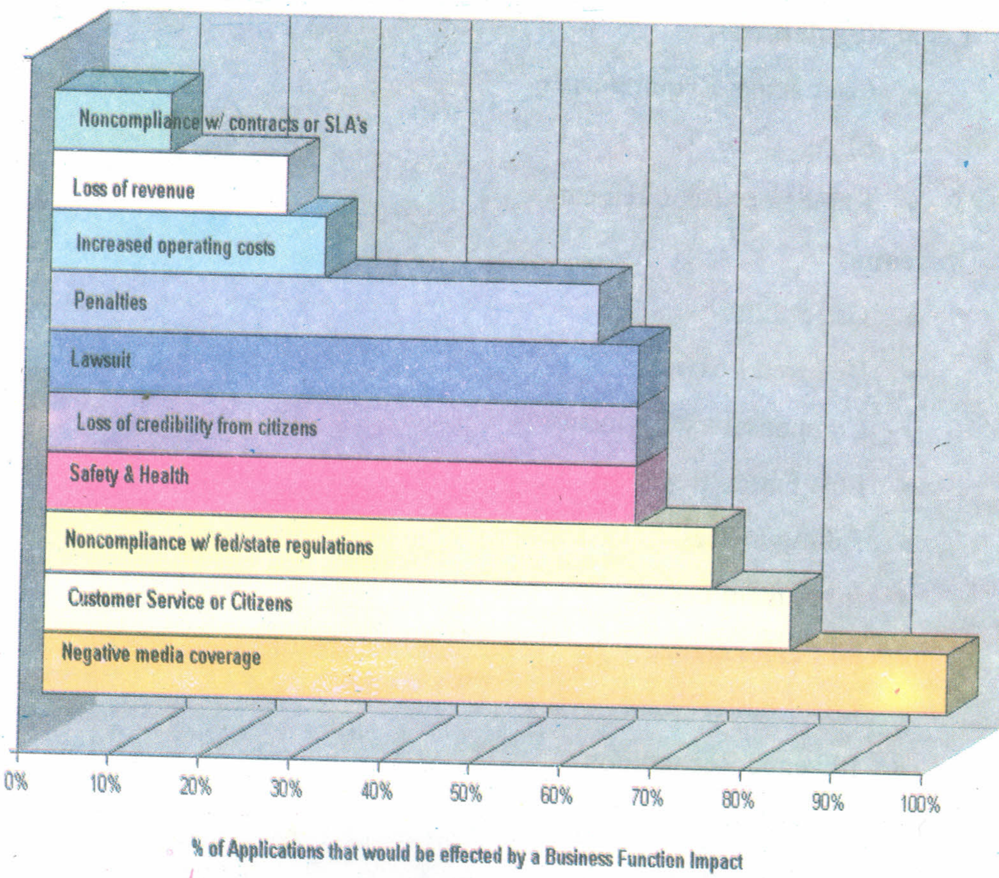


Fig. 2: Customer Responses to Application Business Function Impacts

The benefits using BRP activities are –

PRE EMERGENCY	Increased Sense of Security Reduced Hazard Exposure Reduced Insurance Costs	Improved Organization Image Maintained Or Increased Market Share Improved Customer Loyalty
EMERGENCY	Improved Safety Reduced Damage	
POST EMERGENCY	Reduced Employee Stress Reduced Customer Inconvenience	

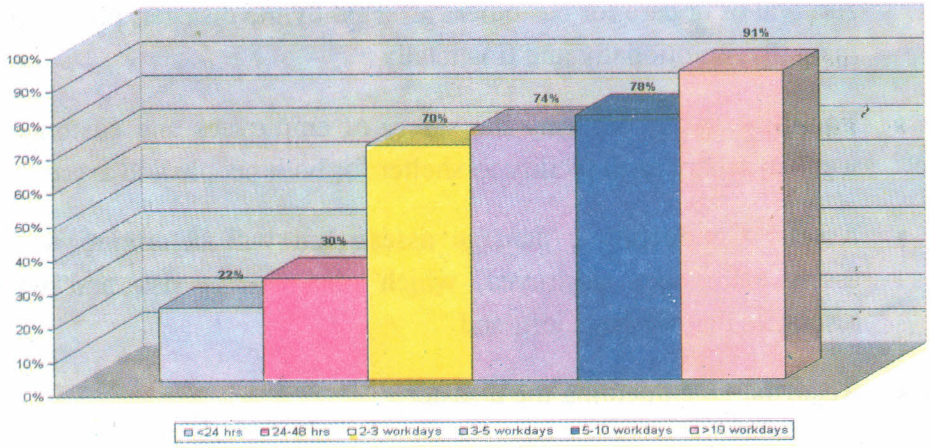


Fig. 3: Customer Responses to Application Service Interruption Duration

2.3 GOAL OF BRP

The goals of disaster recovery and business resumption planning are following:

1. Eliminate or reduce the potential for injuries or the loss of human life, damage to facilities, and loss of assets and records.

   This requires a comprehensive assessment of each department within the business, to insure that appropriate steps have been taken to:

   - Minimize disruptions of services to the business and its customers;
   - Minimize financial loss;

2. Immediately invoke the emergency provisions of Disaster Recovery and Business Resumption Plan to stabilize the effects of the disaster, allowing for appropriate assessment and the beginning of recovery efforts.

   This requires minimize the effects of the disaster and provide for the fastest possible recovery.

3. Implement the procedures contained in the Disaster Recovery and Business Resumption Plan according to the type and impact of the disaster.

   When we implement these procedures, we must prioritize all recovery efforts as follows:

   - **Employees:** Not only must we help to ensure their survival as a basic human concern, but because of their anticipated performance in helping other persons on the business's premises when the disaster strikes

- **Customers:** As we do with employees, we must help to ensure the survival of or care for customers affected by the disaster: physically, mentally, emotionally and financially
- **Facilities:** After ensuring the safety of employees and customers, we then secure each facility as shelter for both people and assets
- **Assets:** Conducting a damage assessment will determine which assets have been destroyed, which ones are at risk and what resources that we have left; and
- **Records:** Documenting the disaster.

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 BRP?

....

....

....

....

2) Explain the effective DR planning stages.

....

....

....

....

3) Write a plan to evaluate the time critical a vities?

....

....

....

....

4) What is the operational consideration in case of some erroneous transactions on the file?

....

....

....

....

2.4 BUSINESS RESUMPTION PLANNING

In case of crisis, the organization will operate through phases of response, resumption, recovery, and restoration. Each phase involves exercising procedures of the BPR The teams associated with the plan represent functions of a department or support functions developed to respond, resume, recover, or restore operations or facilities of the and its affected systems, .Each of the teams is comprised of individuals with specific responsibilities or tasks, which must be completed to fully execute the plan. Primary and alternate team leaders, who are responsible to the plan owner, lead each team.

Each team becomes a sub-unit of organization. Coordination teams may be singular for the organization, whereas technical teams will likely be system specific. Contingency Planning Organizational Chart shows the base organizational structure. The teams are structured to provide dedicated, focused support in the areas of their particular experience and expertise for specific response, resumption and recovery tasks, responsibilities, and objectives. A high degree of interaction among all teams will be required to execute the corporate plan. Each team's eventual goal is the resumption/recovery and the return to stable and normal business operations and technology environments. Status and progress updates will be reported by each team leader to the plan owner

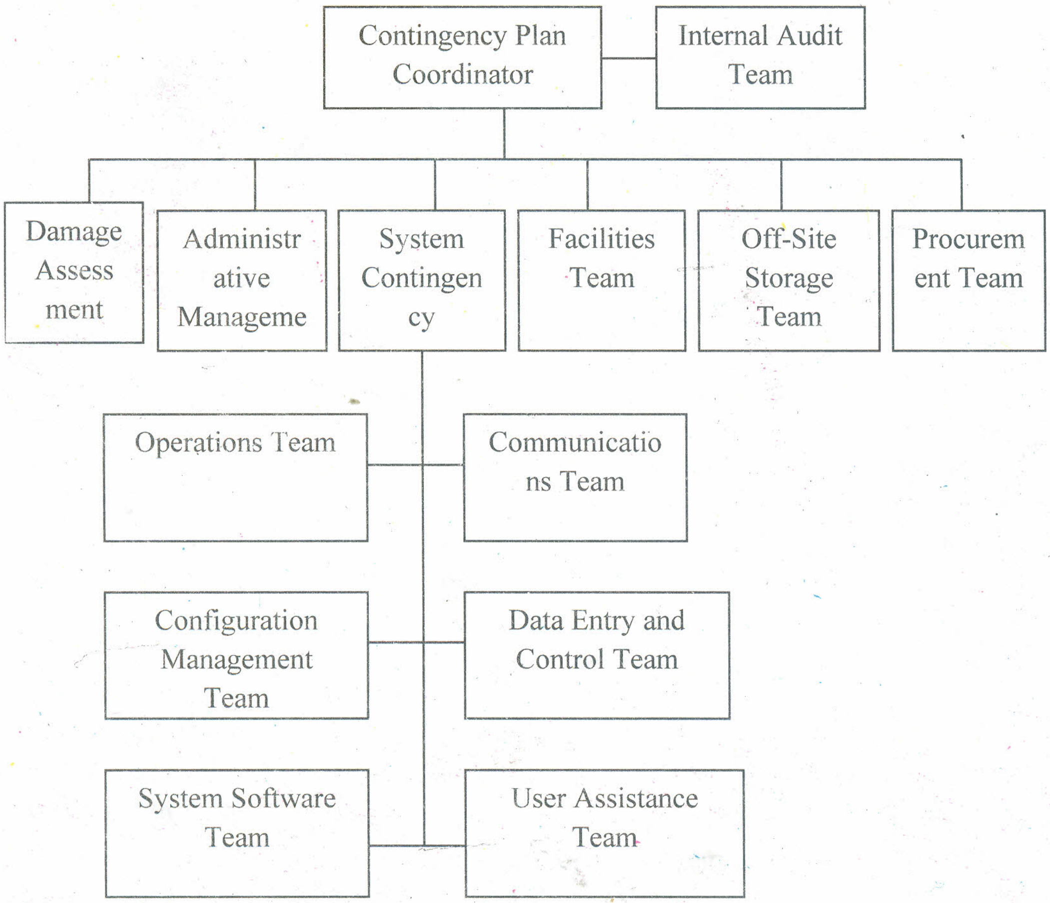


Fig. 4

2.4.1 Checklist

Personnel Checklist	
Have key employees seen the business resumption plan and are all employees aware that there is such a plan? Have employees been told their specific roles and responsibilities if the business resumption plan is put into effect? Have information sessions on the business resumption plan been held? Does your business resumption plan provide a means for replacement staff when necessary?	Does your business resumption plan include home telephone numbers/beeper/cellular phone number etc. of employees with key roles in implementing the plan? [Can you contact them on a 24-hour basis, if necessary, while they are on vacation or otherwise away from the office?] Do designated employees know who does what in the event of an emergency? Have people with special needs been identified and provisions made for them?
Building Premises Checklist	
Consider the condition of your building(s) – old, recently retrofitted or new and the impact this may have on some details of your business resumption plan. Do you have access to a building engineer who can inspect the building and facilities soon after a disaster so that damage can be identified and repaired to make the premises safe for the return of employees as soon as possible? What is the risk of failure of such systems as electrical power, natural gas, toxic chemical containers and pipes? Do you have plans for alternative shelter, if needed?	Is there a plan for the regular inspection of the building(s) and facilities, with an inspection checklist? Are there hazards in adjoining or neighboring buildings that could endanger life or your business/organization? Do employees know where the alternative facilities are located? Are toxic materials safely stored? If public or general transportation is disrupted, will that affect your operations? Has this aspect been considered in your business resumption plan?
Information Technology Checklist	
What arrangements exist for emergency telecommunications? Have provisions been made so that employees can communicate with their families without overloading	How frequently do you test your recovery plan for electronic data processing? For communications during an emergency? Does your business resumption plan incorporate a review of computer

telephone circuits? Is there a plan for alternative means of data transmission if the computer network is interrupted? Is the plan in writing? Are key staff aware of it? has the security of alternative means of transmission been considered?	operations and analyze networking and interdependencies between computers and systems? Are computers protected from leakage from fire sprinklers and pipes on upper floors? Does your business resumption plan consider accessibility to a back-up power generator?
Administrative Procedures Checklist	
Does your business resumption plan cover administrative and management aspects in addition to operations? Is there a management plan to maintain operations if your headquarters is severely damaged or if access is denied or limited for an extended period of time? If some or all of senior management are unable to work, does your business resumption plan have procedures that will enable others to assume these responsibilities? (Is there an executive succession plan?) Is there a designated emergency operations center where incident management teams can co-ordinate response and recovery?	Have essential records been identified? Do you have a duplicate set of essential records stored in a secure and approved location? Are essential records separated for easy retrieval from those that will not be needed immediately? Is there a review procedure to check the protective and emergency devices in offices? (alarm systems, security procedures). Does your business resumption plan include the names and phone numbers of suppliers of essential equipment and other material?
Contracts Checklist	
Do any of your contractors provide a service or deliver goods that are essential to the continued operation of your business/organization and if so, do these contractors have business resumption plans in case they are also affected by the same disruption that has interrupted the functioning of your business? Have alternative sources of supply been established?	

2.4.2 BRP Format

Introduction	
How to use the plan	Plan structure Plan components • Emergency Plan • Recovery Plan

DR Strategies

Commitment	Approval by authority A clear statement of support from senior management.
Objective statement	Government or agency policy stating requirement for resumption plan Objectives to protect lives and physical asserts, minimize disaster impact, activate recovery activities Principles upon which the plan is based
Definition	Ensure consistent terminology throughout BRP plan
Scope	How the agency tackles the plan based on size, geographical spread, organizational structure Limitations/ assumptions
Justification	Risk assessment and impact analysis, including list of main sources of risk and potential impacts on the agency
Emergency Response Time	Agency duty of care to employees
Incident notification and escalation	Identify key appointments Procedure to activate the team Notification process to minimize disruption
Damage assessment	Estimate of damage in disruption duration Damage assessment Maintain accurate, up-to-date, building, floor-room plans, IT infrastructure, etc.
Resumption phase	Summary/ detailed tasks Start time, duration and end time Staff responsibilities and contact details Resources required and contact details Contract information
Media response	Media liaison team calm public fears

Testing schedule	Train staff Schedule continuity activities Test alternative methods
Monitoring and review	Keep plan up-to-date, including maintaining contact lists

2.5 BRP PHASES

The Business Resumption Planning works in different phases in the case of contingency. Each phase address specific functions and responsibilities.

2.5.1 Response Phase

The phase is the starting phase at the immediate state of contingency and the different immediate actions are supposed to initiate.

- To establish an immediate and controlled action at the incident site.
- To conduct a preliminary assessment of incident impact, known injuries, extent of damage, and disruption to the services and business operations.
- To find and disseminate information on if or when access to the facility will be allowed.
- To provide management with the facts necessary to make informed decisions regarding subsequent resumption and recovery activity.

2.5.2 Resumption Phase

After response phase the business resumption phase start where the coordinator are require to execute the plan with the following tasks-

- To establish and organize a management control center and headquarters for the resumption operations.
- To mobilize and activate the support teams necessary to facilitate and support the resumption process.
- To notify and appraise time-sensitive business operation resumption team leaders of the situation.
- To alert employees, vendors and other internal and external individuals and organizations.

2.5.3 Recovery Phase

- To prepare and implement procedures necessary to facilitate and support the recovery of time-sensitive business operations.
- To coordinate with higher headquarters to discern responsibilities that will fall upon Business Operations Recovery Teams and Technology Recovery Teams
- To coordinate with employees, vendors, and other internal and external individuals and organizations.

2.5.4 Restoration Phase

- To prepare procedures necessary to facilitate the relocation and migration of business operations to the new or repaired facility.
- Implement procedures necessary to mobilize operations, support and technology department relocation or migration.
- Manage the relocation/migration effort as well as perform employee, vendor, and customer notification before, during, and after relocation or migration.

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) Assign a priority to each of the "time critical" activities you have identified.

....

....

....

....

2) Determine the minimum needs for response phase.

....

....

....

....

3) List out the BRP Plan that BPO may deploy to avoid loss of data?

....

....

....

....

4) Specific steps in resumption planning?

....

....

....

....

2.6 BRP PROCESS

2.6.1 Find out Critical Activities

Time critical business functions are services and activities whose continued operation is considered essential by management. Non performance would significantly impair the successful functioning of the business.

The following essential mission critical systems/applications/services that must be recovered at the time of disaster in the following order due to critical interdependencies. For example the system has identified the applications and services shown in as mission critical:

SYSTEMS ACRONYM	SYSTEM NAME
Exchange Mail	Microsoft E-mail system
Internet Connectivity	UUNet

2.6.2 Find Out Threats

When developing strategies for a contingency plan, it is helpful to consider the entire range of probable and possible threats that present a risk to an organization. From that range of threats, likely scenarios can be developed and appropriate strategies applied. A disaster recovery plan should be designed to be flexible enough to respond to extended business interruptions, as well as major disasters.

The best way to achieve this goal is to design a contingency plan that could be used to address a major disaster, but is divided into sections that can be used to address extended business interruptions. While each of the identified threats could result in a disaster by itself, in a major disaster several of the threats might be present concurrently or occur sequentially, depending on the circumstances.

As a result, it is advisable to develop several levels of strategies that can be applied as needed.

For example, a localized fire in the computing center may render some of that space unusable. An appropriate strategy for that event may be temporary relocation of personnel to another office within <Name> headquarters or in other suitable local office space in another office building or hotel.. An event that required temporary evacuation of the computer center, such as a truck accident in the tunnel and a chemical spill that may require several days to resolve, may necessitate switchover capabilities and possible regional mirrored redundancy capabilities that would be transparent to the users. An event of greater magnitude, such as an explosion, may render the <Name of headquarters or national office> unusable for an extended duration of time and might necessitate a strategy based on mirrored redundancy as well as a secondary strategy involving a commercial hot site. Time sensitivity and mission criticality in conjunction with budgetary limitations, level of threat and degree of risk will be major factors in the development of recommended strategies.

Risk Analysis Matrix

PROBABILITY OF THREATS			
Probability of Occurrence:	**High**	**Medium**	**Low**
Air Conditioning Failure		X	
Aircraft Accident			X
Blackmail		X	
Bomb Threats		X	
Chemical Spills / HazMat	X		
Cold / Frost / Snow			X
Communications Loss		X	
Data Destruction		X	
Earthquakes			X
Fire	XX		
Flooding / Water Damage			X
Nuclear Mishaps			X

Power Loss / Outage	XX		
Sabotage / Terrorism		X	
Storms / Hurricanes			X
Vandalism / Rioting		X	

IT Threats

Category 1: A single person or group in a Critical Business Unit (CBU) is unable to perform their critical functions.

Category 2: An entire CBU is unable to perform its critical functions

Category 3: Multiple CBUs are unable to perform their critical functions

Category 4: Non CBUs are not able to perform their critical functions

Category 5: A wide spread event that impacts the entire University

2.6.3 Approval Through Management

Gaining the approval and commitment of senior management is essential if resources (personnel, time and money) are to be allocated to the development of a Business Resumption Plan. There are two separate but related reasons why it may be difficult to get management on side and get a business resumption planning program off the ground.

Concept of developing a BRP requires creating an awareness of the risks that an organization faces to justify the costs involved in taking measures to adequately meet that risk. Some idea may be -

- Bring up the idea following a major disaster that has occurred elsewhere. There is usually a heightened sense of awareness following such events and willingness to undertake these types of actions.
- Complete a risk assessment to demonstrate the level to which the organization is at risk
- Reinforce the risk assessment with statistics on business and disaster.
- Use graphic examples such as scenarios to illustrate vulnerability to various hazards.
- Include cost estimates for losses of both capital investments and sales.

2.6.4 Develop A BRP Plan for the Organization

The development of a Business Resumption Plan is to ensure the continuity of services and the ongoing success of the organization in emergency situations. The best way to plan the BRP is the people who perform a job on a regular basis. BRP Policies will allow them to resume essential activities following an unplanned business interruption. Each part of the organization must deal with what must be done to recover the essential activities if staff are incapacitated, information are lost, facilities or assets destroyed or rendered inaccessible. Each section of the plan should stand alone. The plan for each part of business and the final plan for the business as a whole should incorporate the cost of implementation in terms of personnel and financial resources. BRP plan should also cover staffing requirements such as replacement personnel, extraordinary staff expenses and health and safety factors.

2.6.5 Communicate BRP Plan to the Employee

Since the development of a Business Resumption Plan ideally involves all employees, they should be made aware of the policy, that such a program is to be undertaken and what can be expected of them during the process. Therefore once senior management has completed a BRP Policy this commitment should be relayed to all employees via memo, information sessions, etc. The initial information should include:

- Policy statement
- Explanation of BRP
- Being undertaken
- Ensure economic security of the organization and it is membership
- Expectation from various groups

Possible information could include:

- Names of the BRP coordinator and planning team
- Framework details
- Progress reports

2.6.6 Test the BRP Plan

Conduct a test of the plan in a realistic fashion and with ample warning to all employees that the plan is being tested. If you don't test the plan you risk not having it work in a real emergency situation. The plan can be tested in stages, or levels ranging from the "table-top exercise" to a full scale simulation of a post-disaster situation.

Desk top walk through: Prior to any detailed testing, key stakeholders in the BRP are convened in a conference room, and a detailed review is performed of the plan. Many small events are described and the participants are asked to state how the plan would guide their reactions. The events should require utilization of: major backup resources, emergency operations approaches, and all emergency response teams. Following this step, operations and simulation tests are scheduled.

Operational testing: Few organizations operationally test the complete disaster reaction cycle of: activation, life-safety, damage assessment, mobilization, emergency operations using off-site files and backup resources, and recovery planning. Only the data processing emergency operations area can be tested without involving a substantial number of persons during business hours. The scope of most operational tests therefore, includes: a semi-annual off-hour call to the manager of data center operations, assembly of the backup site operations team, acquisition of backup materials from an off-site location, travel to a backup hot/cold site, installation of systems and applications software, loading production data, and systems test of several critical applications.

Simulation testing: Simulation is the most feasible approach for testing the decision making aspects of disaster reaction activities. The use of simulation exercises for BRP has been spreading slowly over the last decade. Unlike their counterpart military war games that use computer driven scenarios to perform very realistic exercises, BRP exercises are paper and pencil simulations. Teams are placed at tables representing their backup locations, and the description of an evolving disaster is presented. The teams communicate using backup communication resources or forms, make decisions, and everyone pretends that what is ordered actually happens. Debriefings and evaluation studies follow to correct any flaws in the BRP.

2.7 REVIEW THE BRP PLAN

Review business resumption plan on a regular basis. Update it to reflect changes in activities, procedures, performance, etc. The business resumption plan allows not only for a rapid resumption of services to clients, but also makes efficient use of resources. To do this the BRP re-establishes functions on a priority basis. Before the actual writing of the BRP can begin the planning team will need to facilitate background research into two areas: To determine the priority of re-establishment of organization functions and to determine the minimum resource requirements necessary for these functions to be performed.

The business resumption plan allows not only for a rapid resumption of services to clients, but also makes efficient use of resources. To do this the BRP re-establishes functions on apriority basis. Before the actual writing of the BRP can begin the planning team will need to facilitate background research into two areas: To determine the priority of re-establishment of organization functions and to determine the minimum resource requirements necessary for these functions to be performed.

The operational review is a three step process:

1. Prioritize organizational outputs (The goods or services produced by the organization as a whole) largely on the basis of the impact to the organization's clientele.

2. Based on the results of the above step, prioritize the re-establishment of the department level functions required to support the organizational outputs as identified above and;

3. A determination of the types and amounts of resources that will be necessary to maintain the department level functions identified.

Organizational Elements

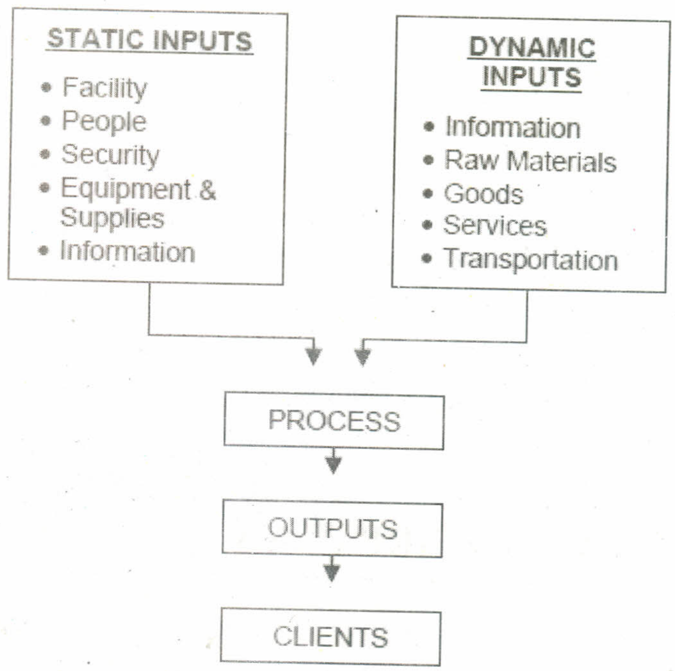


Fig. 5

2.7.1 Organizational Outputs

Senior management, the BRP coordinator and the planning team should meet to assign priorities for the recovery of organizational outputs.

A. Outputs of the Organization

List (name and describe) the outputs provided by the organization as a whole to its clients. These may include:

- Services
- Programs
- Products

This information will largely be the result of the knowledge of the planning team but can be sourced from legislation, annual reports, strategic plans or other documents held by the organization.

List Organizational Outputs

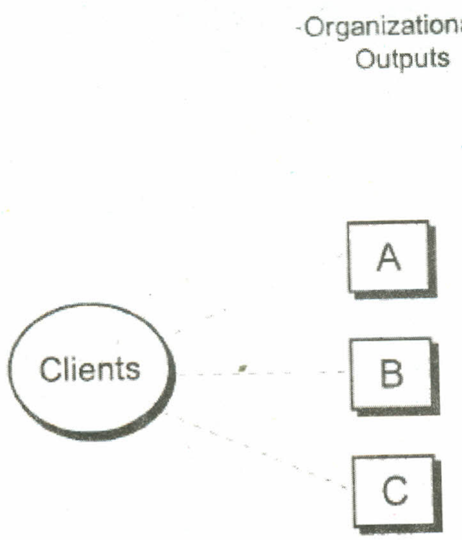


Fig. 6

B. Evaluate and Prioritize Organizational Outputs

From the list that has just been created, senior management and the planning team should evaluate the degree of importance of each organizational output. This involves describing and estimating the likely impact of loss or delay of that output and approximating the length of time that the output could be down before the organization would begin to experience serious adverse effects.

Tangible Impacts

- Financial
- Legal and contractual liability
- Effects on other departments
- Safety and security of the public or personnel etc.

Intangible Impacts

- Public image
- Client confidence and support
- Employee morale, etc...

From the evaluation assign categories for restoration of each output. To help put impacts in perspective consider each output from a client point of view. As a client how long am I willing to be without a particular product or service, what will the effects of that loss or delay is and how will it impact my perception and future relationship with the provider of the product or service?

Evaluate and Prioritize Organizational Outputs

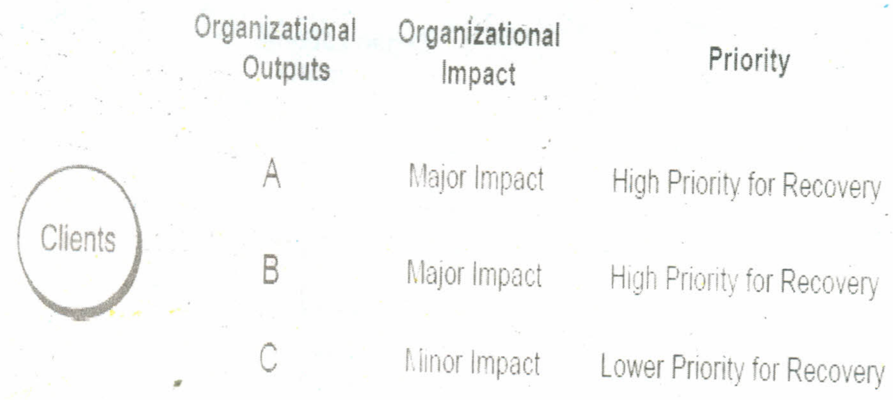


Fig. 7

Explanation

- Loss of A and B constitute a major impact to the organization and are assigned priority for recovery
- Loss of C is not as critical and receives a lower priority

Organizational Outputs Worksheet (Sample)

OUTPUT #	DESCRIPTION OF OUPPUT	EFFECT OF LOSS OF OUTPUT	TIME TO REESTABLISH	IMPACT
				NONE MINOR MODERATE MAJOR
				NONE MINOR MODERATE MAJOR
				NONE MINOR MODERATE MAJOR

2.7.2 Department Level Functions

Once organizational outputs have been prioritized it is necessary to identify the department level functions that support the organization's ability to produce and deliver goods or services.

A. List Department Functions

Planning team members should return to their respective departments and, over a period of several weeks, consult with staff to compile a list of department functions (the operational. responsibilities, tasks and processes for that department)

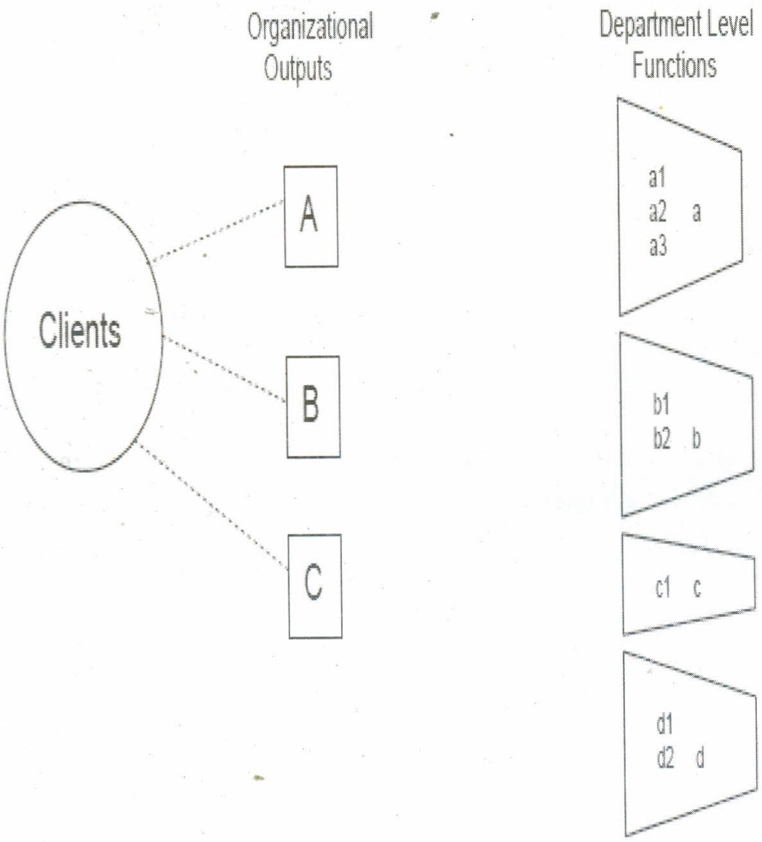


Fig. 7

B. Evaluate Departmental Linkages

After listing all department's functions consider the types and relative strengths of relationships that the individual department functions have with each other and with the outputs of the organization as a whole (Fig. 8). The difficulty of this process will vary depending on the size and complexity of the organization.

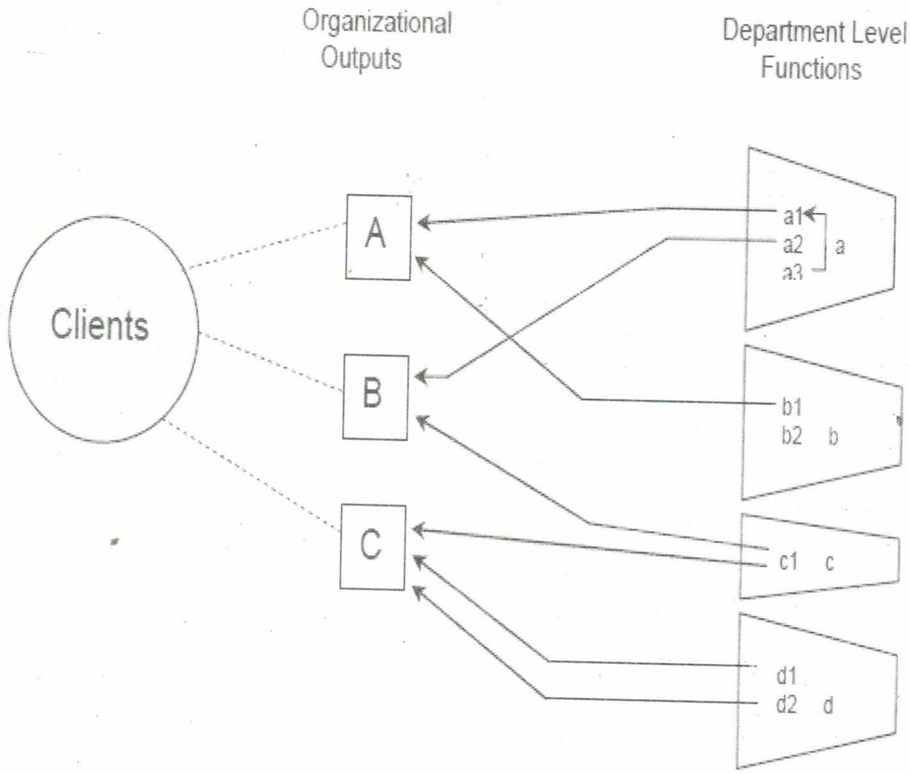


Fig. 8

C. Evaluate and Prioritize Department Functions

With the list of departments functions and their interrelationships, the planning team and senior management should again meet to assign priorities to the re-establishment of departmental functions .

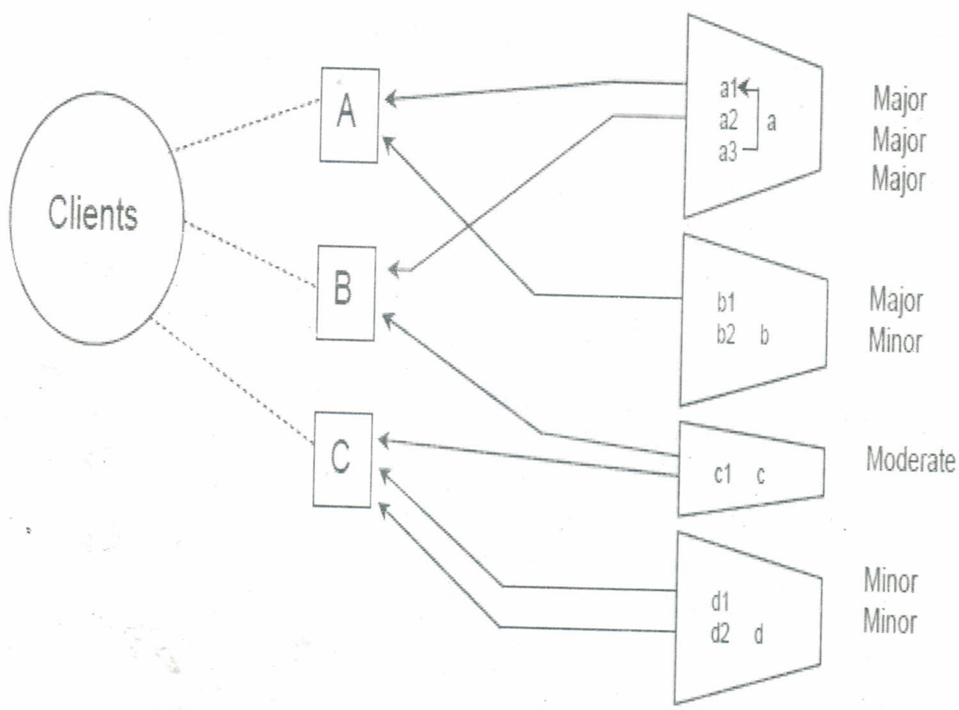


Fig. 9

Explanation

Lines with arrows indicate functional relationships

Function a1 depends on a3

Output A requires input from functions a1 and b1

Output B requires input from functions a2 and c1

Output C is not essential so functions d1 and d2 are not critical and c1 remains essential only to output B

Therefore

Department a - All functions receive top priority

Departments b and c have a high priority

Department d receives lower priority. Personnel may be temporarily reassigned to other tasks or duties

2.7.3 Determine Resource Needs

Planning team members should meet with their departments to determine the minimum resource requirements necessary to maintain department functions.

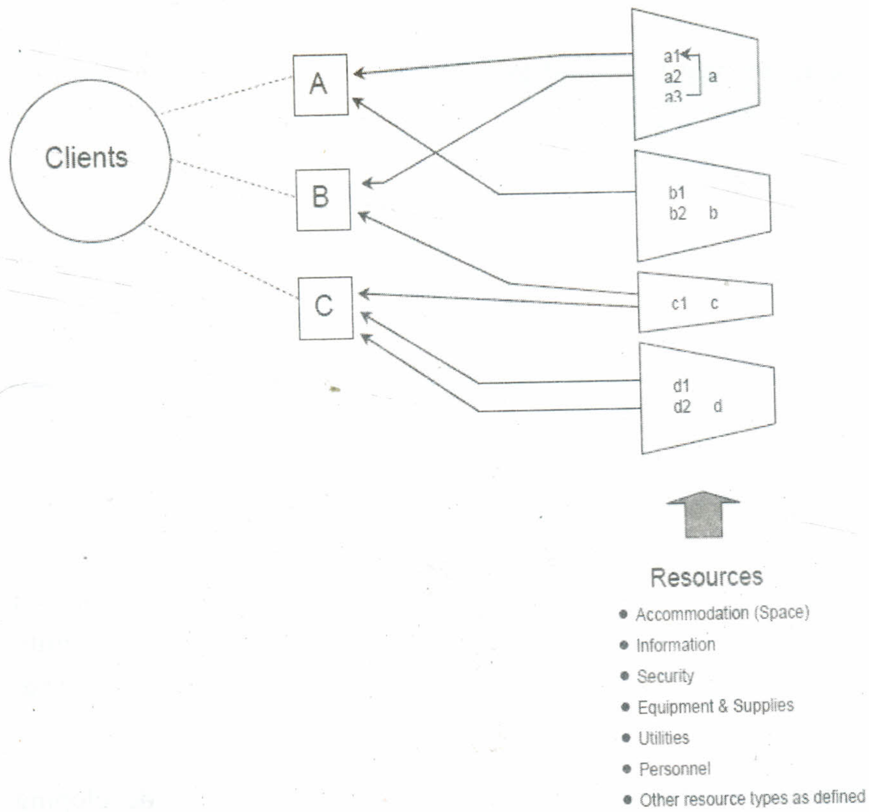


Fig. 10

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) Discuss different data risk on the internet.

....

....

....

....

2) Explain the different prevention techniques for data risk on the internet.

....

....

....

....

3) What are the different methods to reduce the impact of risk?

....

....

....

....

4) List out the major steps to review the BRP Plan.

....

....

....

....

2.8 LET US SUM UP

A Business Resumption Plan (BRP) is a plan activated during or immediately after an emergency and is aimed at permitting the rapid and cost effective resumption of an organizations essential operations in order to maintain continuity of services to it's clients. It sets the stage for, but is a separate entity from, long term disaster recovery which returns the organization to normal operating conditions.

The first phase requires obtaining senior management commitment; developing and communicating, a BRP policy and assembling a team to develop the plan. The plan is based on information from a review of the business activities that support the organizations products and services. The results of this step are a determination of the order of restoration of business functions and the resources required to support each of these functions. The third phase is the actual writing of the business resumption plan. This involves using the information from the previous step to develop a recovery structure that meets the needs of the organization, staffing the structure, assigning planning responsibilities one of which is the development of activity sheets for all key players which is the backbone of the BRP. The fourth phase includes writing other components of the plan and combining these with the activity sheets into a plan. The fifth and final phase is the implementation and maintenance of the BRP. Implementation includes gaining management approval and training staff in the content and their roles in the plan. Maintenance requires that the plan be properly stored, tested and updated so that it is a current and effective tool for responding to the effects s of a disaster.

The inability of an organization to recover its ability to deliver goods and services in a timely and cost effective manner typically results in significant financial stress and often leads to the failure of the organization. Business Resumption planning as demonstrated is an effective tool in maintaining continuity of services and substantially increasing the odds of an organization surviving a disaster.

2.9 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

1) Business Resumption Plan (BRP): The BRP addresses the restoration of business processes after an emergency, but unlike the BCP, lacks procedures to ensure continuity of critical processes throughout an emergency or disruption. Development of the BRP should be coordinated with DRP (Disaster Recovery Plan) and BCP (Disaster Recovery Plan).

2) An effective DR plan consists of the following stages:

   - Programme description
   - Pre-planning activities (project initiation)
   - Vulnerability assessment and general definition of requirements
   - Business impact analysis
   - Detailed definition of requirements
   - Plan development
   - Testing programme
   - Maintenance programme
   - Initial plan testing and plan implementation.

3) Time critical business functions are services and activities whose continued operation is considered essential by management. Non performance would significantly impair the successful functioning of the business. Consider the following as they apply:

   - What functions would have to be done immediately after a business interruption? What could be postponed?
   - What are your external requirements on a day-to-day basis? What do you need from outside your business in order to continue to function?
   - How long can your essential business functions be inoperative?
   - Are there regulator requirements or penalties that must be considered if you cannot fulfill your obligations due to unplanned business interruption?
   - What are the costs to respond vs. the short-term loss of revenue?
   - Are other organizations dependants on functions that your business performs? What are your external outputs?

4) If we are notified in advance that a file contains errors, it would be returned without posting and a new file requested. If we are notified of the errors after the file is posted we would manually reverse the errors, or request the originator to send reversal postings, or request our software vendor to assist with reversing the entries. It would depend on what the errors are and how many errors there are.

Check Your Progress 2

1) priority to each of the "time critical" activities

   i. less than one day Priority 1
   ii. 2 to 4 days Priority 2
   iii. 5 to7 days Priority 3
   iv. 8 to10 days Priority 4
   v. more than 10 days Priority 5 etc.

2) The ability to communicate with employees, suppliers, customers, etc. is the key aspect to an effective initial response. The minimum needs for initial response.

   - List essential information sources (operating instructions, manuals, databases) and alternate sources for this information.

- List essential equipment needs (telephones, computers, etc.) and sources of alternative equipment. Have support services been considered?

3) BPO had developed and deployed various BRP methods so as to minimize the loss in unavoidable circumstances, if any. Some of them are listed as follows:

   a) **Data Backup Practice:** BPO have stringent policy to take regular Data Backup so as to avoid unpleasant circumstances. Network Administrators use hard disk image computer backup solution on daily basis. Backups are useful primarily for two purposes: to restore a computer to an operational state following a disaster (called disaster recovery) and to restore small numbers of files after they have been accidentally deleted or corrupted.

   b) **FTP Maintenance:** BPO has Dedicated Servers providing FTP facility with Backup and Recovery Strategies. BPO also conduct a weekly remote backup to provide a failsafe version. Even if the data-center burns down, BPO will have a copy of data. BPO use Secured Shell Layer tool for FTP Security, effective for Selecting User IDs and Passwords.

4) The process of resumption plan development draws on information already gathered in the risk management process and emergency response planning. The following steps should provide guidance in plan development, implementation and ongoing maintenance. These steps are not exhaustive, and will not necessarily apply to every directorate or business unit.

   - List the major services or functions in this area of responsibility (agency, division, branch, directorate, group)
   - Rank services and functions
   - Assign a priority to each function or service
   - Develop a planning objective and target recovery timeframe for each service or function
   - Determine minimum needs for initial resumption
   - Obtain senior management approval for proposed approach
   - Delegate planning assignments to the staff who carry out the critical services and functions on a day-to-day basis
   - Write the detailed plan

Check your progress 3

1) Security risk can be categorized as follows:-

a) **Data privacy and confidentiality risk**

Data may be monitored and read by unauthorized parties.

b) **Data integrity risk**

Data may be altered or modified by unauthorized parties with malicious intent, thus compromising the insurer's databank and may affect the accuracy of product information, integrity of transactions and impact customers' confidence.

c) **Authentication of users risk**

The anonymity of users in cyber space, including that of customers and the insurer renders risk in the authenticity of the parties to a transaction as to whether the parties are who they say they are.

d) **Repudiation risk**

Customers may dispute the validity of, or refuse to acknowledge legitimate communications or transactions.

2) Prevention techniques:

- User IDs and Passwords
- Personal and policy details
- Time stamping - Successful policy statements for purchases and renewals should be time stamped to prevent backdating of documents and renewal records.
- Reconciliation- The insurer should perform daily reconciliation of all successful transactions with the payment transaction statements provided by the relevant bank.
- Segregation of roles and responsibilities
- Testing

3) The different methods to reduce the impact of risk are:

- building design features, engineering and structural barriers;
- separation or relocation of an activity and resources;
- off-site storage of documents and computer data;
- contractual arrangements with conditions which make proper provision for disruption to services;
- contingency plans (emergency response and resumption plans);
- emergency response procedures, including removal, containment or suppression of the source of risk and/or removal of elements at risk, *ie* evacuation of staff, retrieval of essential records;

- resumption strategies;
- public relations; and
- *ex-gratia* payments

4) The major steps in BRP Review plans are:

- Organizational Outputs
- Department Level Functions
- Determine Resource Needs

2.10 SUGGESTED READINGS

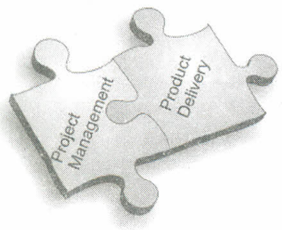
- Business Resumption Planning for the Management Team, Human Resources Development Canada
- Daley, Wayne (1991), Business Resumption Planning: An Answer to Surviving a Disaster, Emergency Preparedness Digest July - September 1991
- http://datasure.com/dbft.html
- World, Geoffrey (1992), The Disaster Recovery Planning Process, Disaster Recovery Journal Systems Support Inc. St. Louis

UNIT 3 PLAN TEMPLATES AND SOFTWARE TOOLS

Structure

3.0 Introduction
3.1 Objectives
3.2 Project Management
3.3 What is a Template?
3.4 Importance of Project Management
3.5 Getting Started with MS-Project
  3.5.1 Defining the Project
  3.5.2 Defining a Timeline
  3.5.3 Tracking Progress of the Project
  3.5.4 Managing the Project Resources
3.6 Step by Step Process
3.7 Let Us Sum Up
3.8 Check Your Progress: The Key
3.9 Suggested Readings

3.0 INTRODUCTION



Project Management

Project management is a carefully planned and organized effort to accomplish company's objectives, for example, manage marketing activities, manage multi team's tasks and control work processes in multi location environment. Good project management templates and software's will ensure mechanisms and control elements like reports and dashboards to ensure activities and tasks completion or alert mechanisms to implement recovery actions where necessary.

Project management includes developing a project plan, defining and confirming the project goals and objectives, identifying tasks and how goals will be achieved, quantifying the resources needed, and determining budgets.

Project management is a complex undertaking, with many stages and processes. It should follow the full business lifecycle, from definition and justification of the project, through to delivering demonstrable benefits for the business.

3.1 OBJECTIVES

After studying this unit, you should be able to:

- define Project Management;
- explain importance of Project Management;
- define a Project in MS-Project;
- define Timeline;
- explain Tracking progress of the Project; and
- managing the Project resources.

3.2 PROJECT MANAGEMENT

It is the discipline of planning and organizing resources to bring about the successful completion of specific goals while managing constraints of scope, costs and time.

Cost is everything that has to do with money. It is composed of several variables: people, materials, equipment, profit, etc.

Time expended for the project is the sum of all the time units taken to accomplish the tasks that lead to the production of a deliverable.

Scope also called specifications, is the definition of what the final results are supposed to be. Quality is a major component of scope. A well-managed project, one that delivered what it was supposed to, within the specified timeframe and without spending more money than it was allocated.

3.3 WHAT IS A TEMPLATE?

A template provides the basic framework of a project that was previously used in the system or from a project that was imported from MS-Project. All fields and data are maintained when a project is saved as a template.

You can save your project plan as a template of which you could use at a later stage for other project plans.

Working with a Project plan template is powerful by providing structure for project managers and uses project plan best practices to start effectively managing projects.

The Templates subsystem allows you to navigate and update the list of project templates that have been saved to the project database. You can also share your thoughts and ideas on specific templates by taking advantage of the Notes and Posts section.

3.4 IMPORTANCE OF PROJECT MANAGMENT

Projects are the means to achieve business objectives. They, along with ongoing operations represent the activities that make organizations run. They deliver the goods and services that satisfy customers and owners. All organizations have projects. A project may be a large task or a complex activity, in fact, any work that is done to achieve an objective on time and within budget.

When you change the way people work, you are managing a project. When you launch a new product you are managing project. Projects are ideas in motion. They may be efforts to move an office full of people to another location, put on an event, merge two organizations, institute a new training program, put together a budget, create a new product, change or produce a web site, put a new process into place, etc.

More and more people recognize that their ability to effectively manage projects is now key to their success within the organization. The ability to better manage projects is a way to achieve the edge over competitors and deliver greater value to owners and customers.

Project management is a complex discipline. It requires years of hands-on experience and of study. There are techniques to learn and tools to master.

Microsoft Project software is one of those tools.

3.5 GETTING STARTED WITH MS-PROJECT

Before embarking on the project you need to put down a few key points very clearly:

1. Conceptualize and identify the purpose of the project
2. Define its objectives
3. Finalize its scope
4. Identify its activities
5. Assign resources to activities
6. Create an estimate of time and costs
7. Make honest assumptions about various relevant factors that can affect the duration of a project and its costs
8. Discuss alternative scenarios and build contingency plans.

3.5.1 Defining the Project

You can create a Project from a Template File by choosing File > New from the menu. In the New File dialog box that opens, select the Project Templates tab and select the template that suits your project best and click OK. Start by defining the properties of the project that you are going to manage.

Now, you need to define for Microsoft Project the start or ending date for the project. If you fill in a start date, Project schedules your tasks from that date, based on the order in which tasks need to be completed and the availability of resources assigned to work on each task. But, if you have to finish the project by a deadline date, you can enter the finish date too. All intermediate schedules will then be set by Project.

Start Date: The date when a task is scheduled to begin. This date is based on the duration, calendars, and constraints of predecessor and successor tasks. A task's start date is also based on its own calendars and constraints.

Once a new Project page is opened, the Project Information dialog box opens. You need to know the start date and the basic operating rules of the organization.

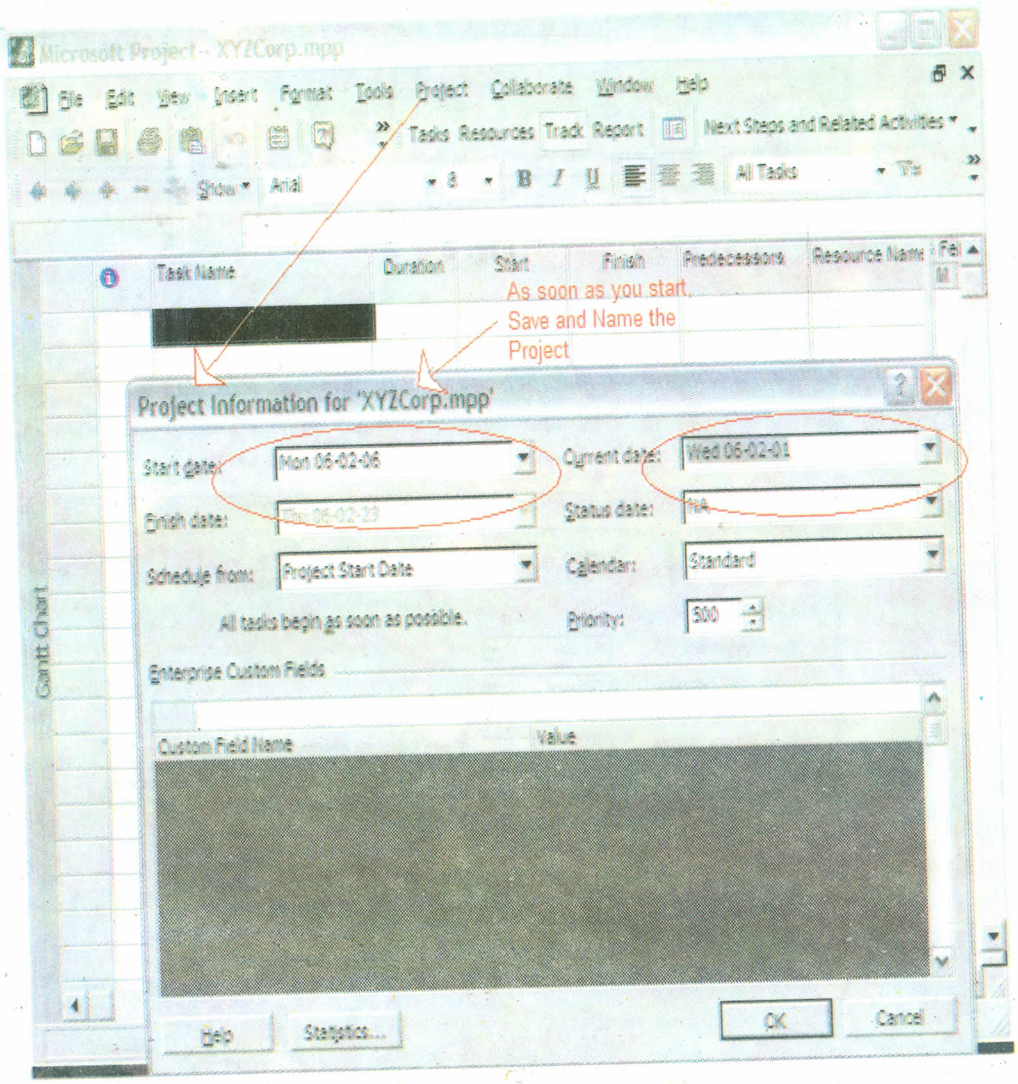


Fig. 1

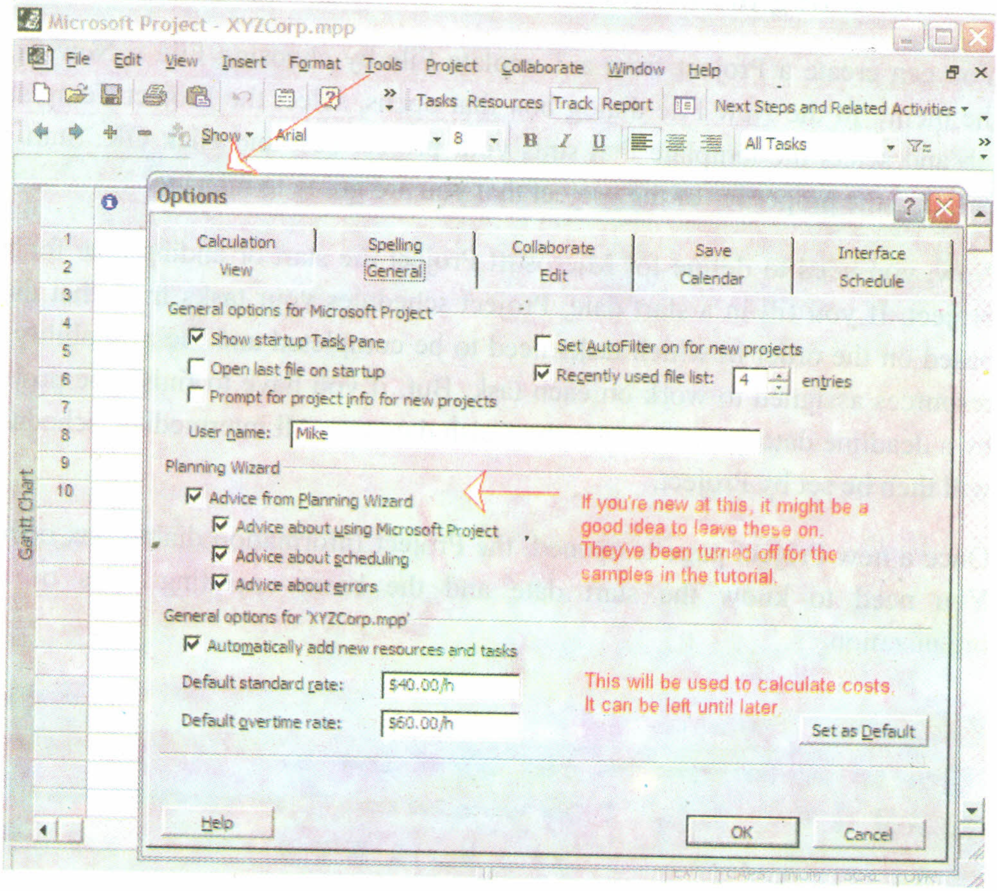

Microsoft Project - XYZCorp.mpp
File Edit View Insert Format Tools Project Collaborate Window Help
Tasks Resources Track Report Next Steps and Related Activities
Options
Calculation Spelling Collaborate Save Interface
View General Edit Calendar Schedule
General options for Microsoft Project
Show startup Task Pane
Open last file on startup
Prompt for project info for new projects
Set AutoFilter on for new projects
Recently used file list: 4 entries
User name: Mike
Planning Wizard
Advice from Planning Wizard
Advice about using Microsoft Project
Advice about scheduling
Advice about errors
If you're new at this, it might be a good idea to leave these on. They've been turned off for the samples in the tutorial.
General options for 'XYZCorp.mpp'
Automatically add new resources and tasks
Default standard rate: $40.00/h
Default overtime rate: $60.00/h
This will be used to calculate costs. It can be left until later.
Set as Default
Help OK Cancel

Fig. 2

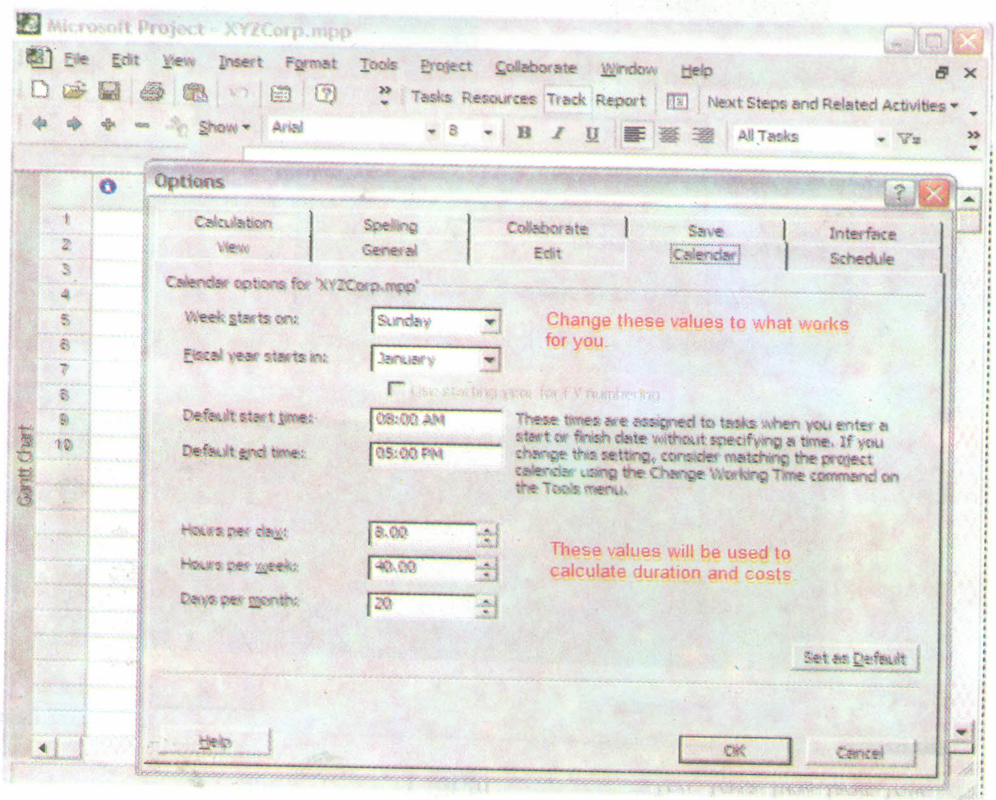

Microsoft Project - XYZCorp.mpp
Options
Calculation Spelling Collaborate Save Interface
View General Edit Calendar Schedule
Calendar options for 'XYZCorp.mpp'
Week starts on: Sunday
Fiscal year starts in: January
Change these values to what works for you
Default start time: 08:00 AM
Default end time: 05:00 PM
These times are assigned to tasks when you enter a start or finish date without specifying a time. If you change this setting, consider matching the project calendar using the Change Working Time command on the Tools menu.
Hours per day: 8.00
Hours per week: 40.00
Days per month: 20
These values will be used to calculate duration and costs
Set as Default
Help OK Cancel

Fig. 3

First: break the whole project into individual tasks.

This may not be as easy as it sounds. You want the tasks to be small enough to be manageable but, not so small as to involve the atomic level. This will draw on the experience of the project manager.

Normally, a task involves one person or a small group of people over a span of time that can be measured in days.

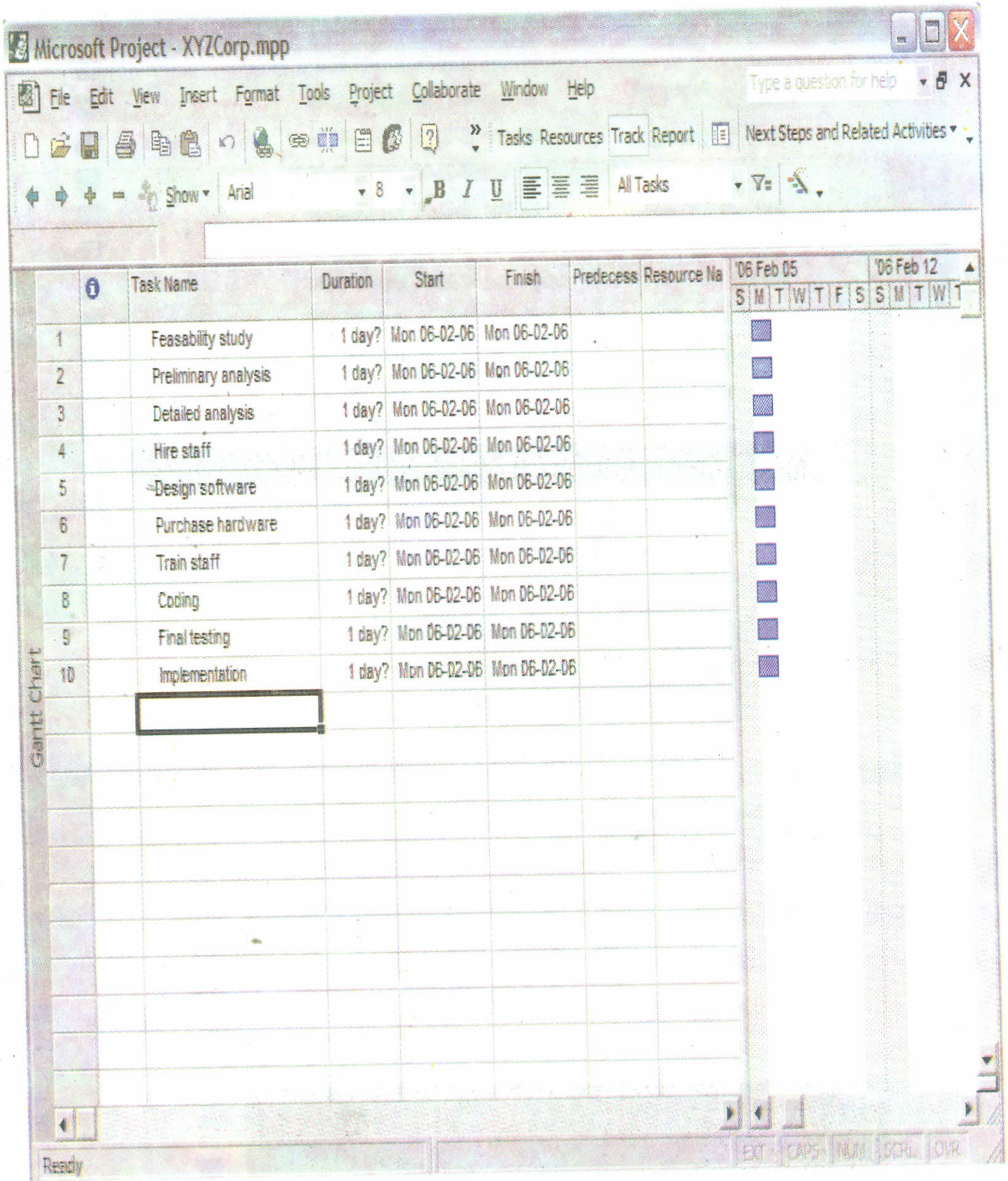


Fig. 4

Don't worry that the tasks all last 1 day and start on the same day. We'll get to that later.

Now, you will probably want to group tasks under phases.

In MS Project, grouping is done from the top down with Final total at the very top, with Subtotals below and so on.

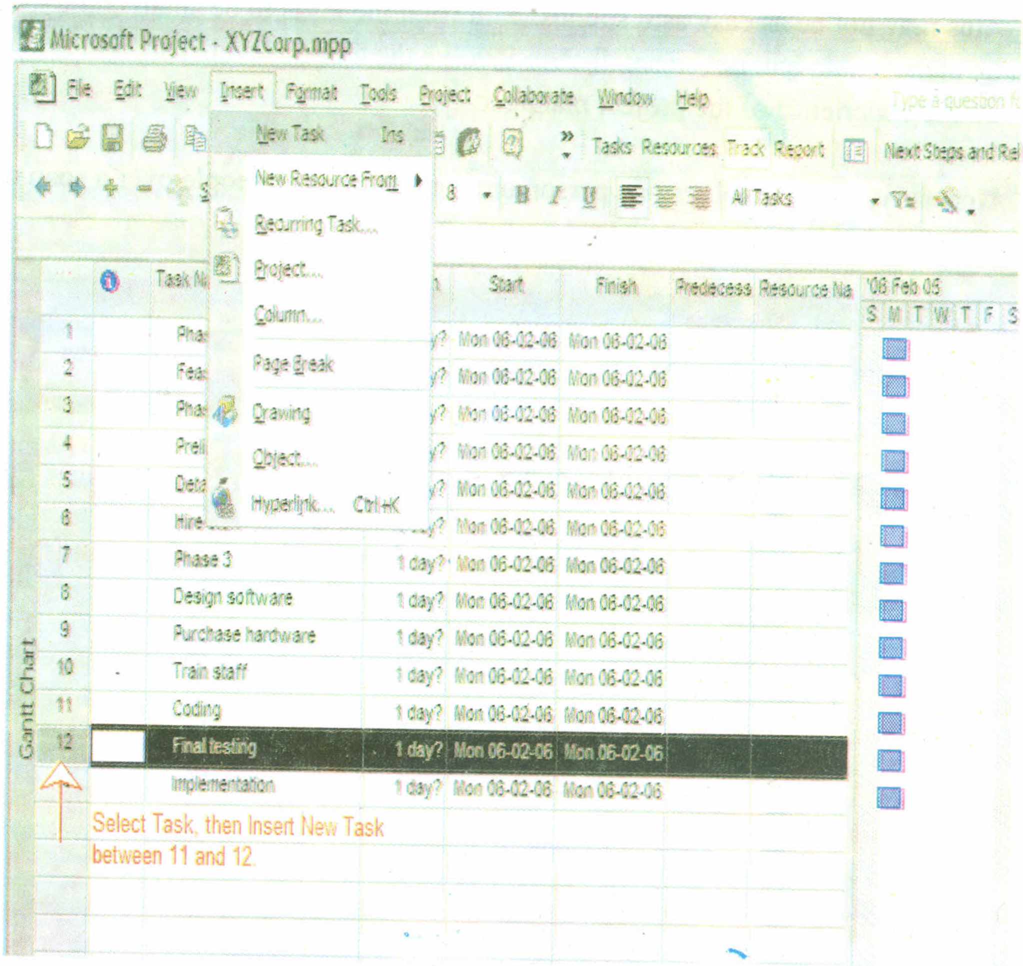


Fig. 5

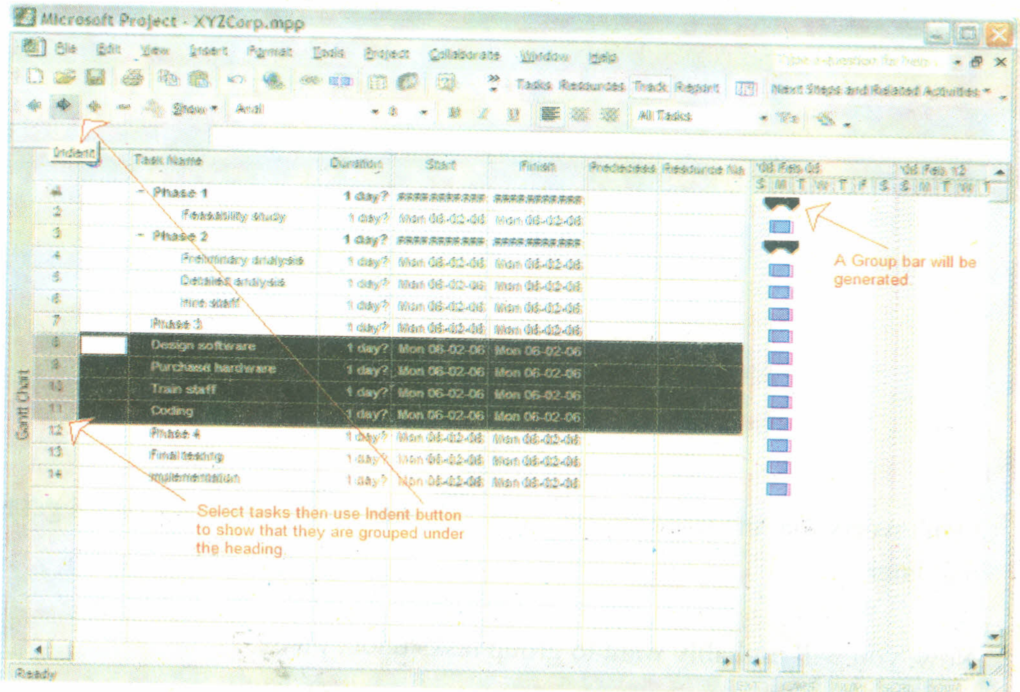


Fig. 6

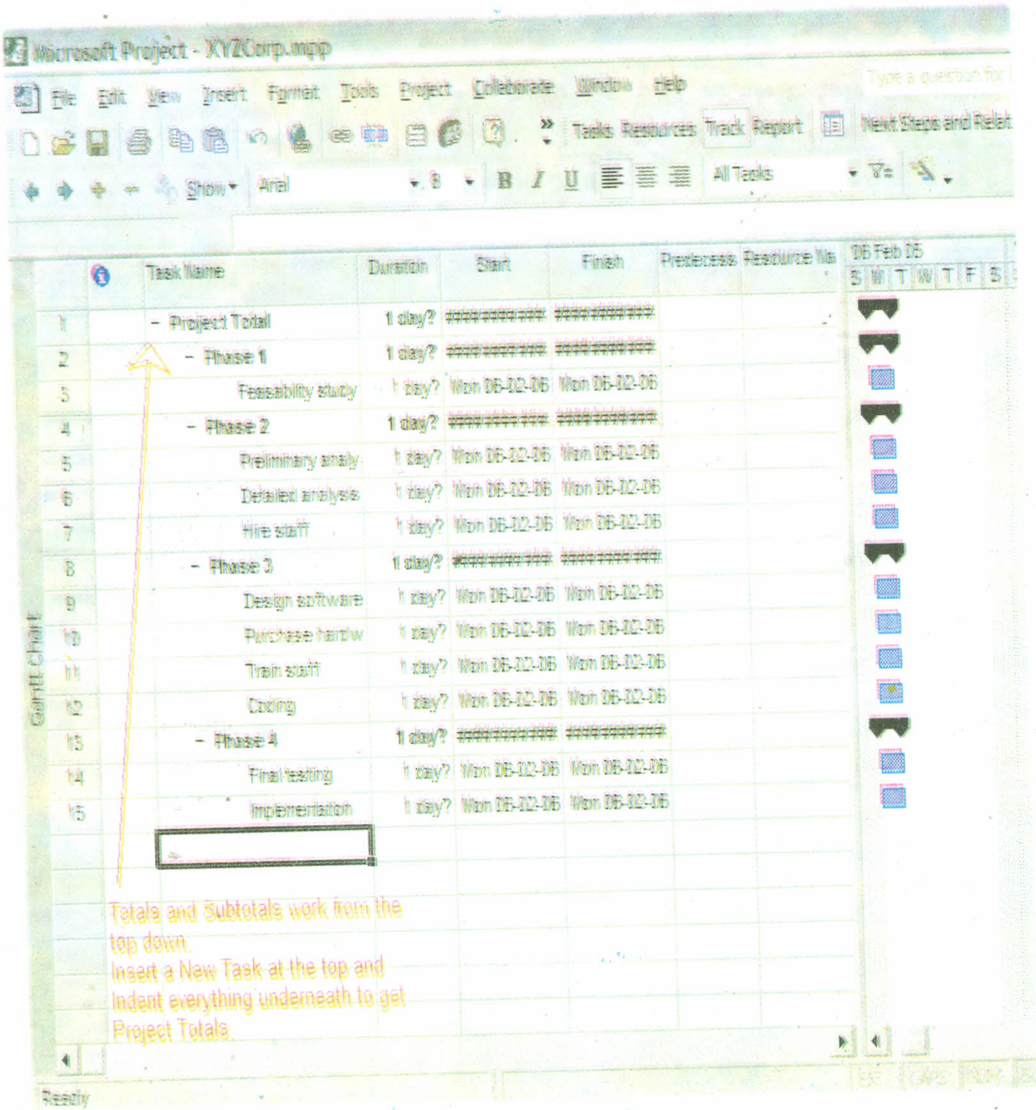


Fig. 7

3.5.2 Defining a Timeline

The next step is to define the duration of all the tasks.

Again, you will draw upon the experience and knowledge of the project manager and the participants.

You want to obtain a value that is as realistic as possible for the duration of each task.

That may have to be negotiated.

If there's disagreement, a simple formula to establish a value has been around for years:

find an optimistic value, D(o), a pessimistic value, D(p) and a realitic value, D(r) .

Then: Duration = (D(o) + D(p) + 4 x D(r)) / 6

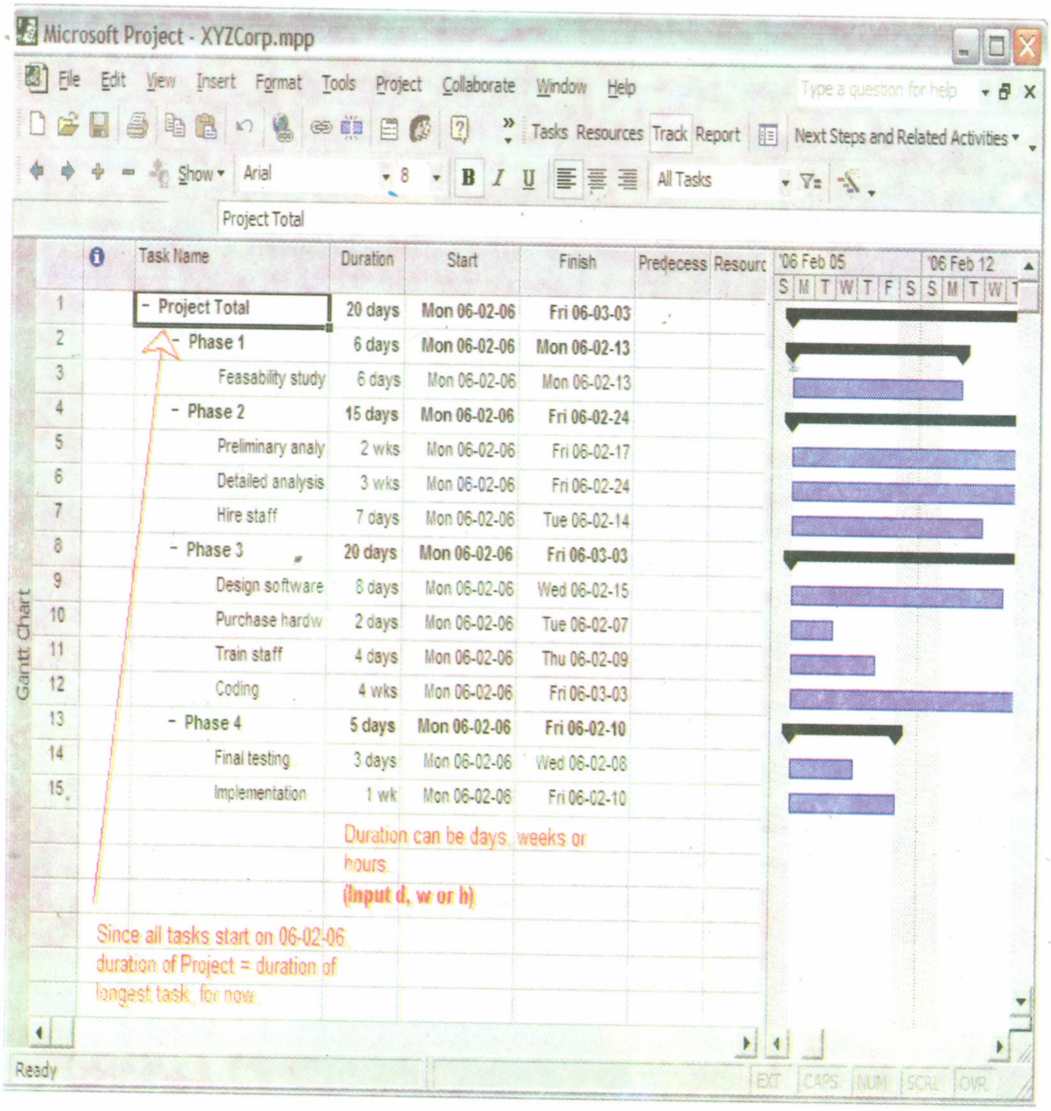


Fig. 8

You now have duration for each of the tasks but they all start on the same day.

Obviously, you will have to specify the sequence of the tasks and the links between them.

In MS Project a task that must be completed before another task can start is called a **predecessor**.

The first task has no predecessor and each of the following tasks has to have at least one.

In some cases a task may have several predecessors meaning that several tasks have to be completed before that one can start.

In other cases a task may be predecessor to several others - its completion can allow several other tasks to start.

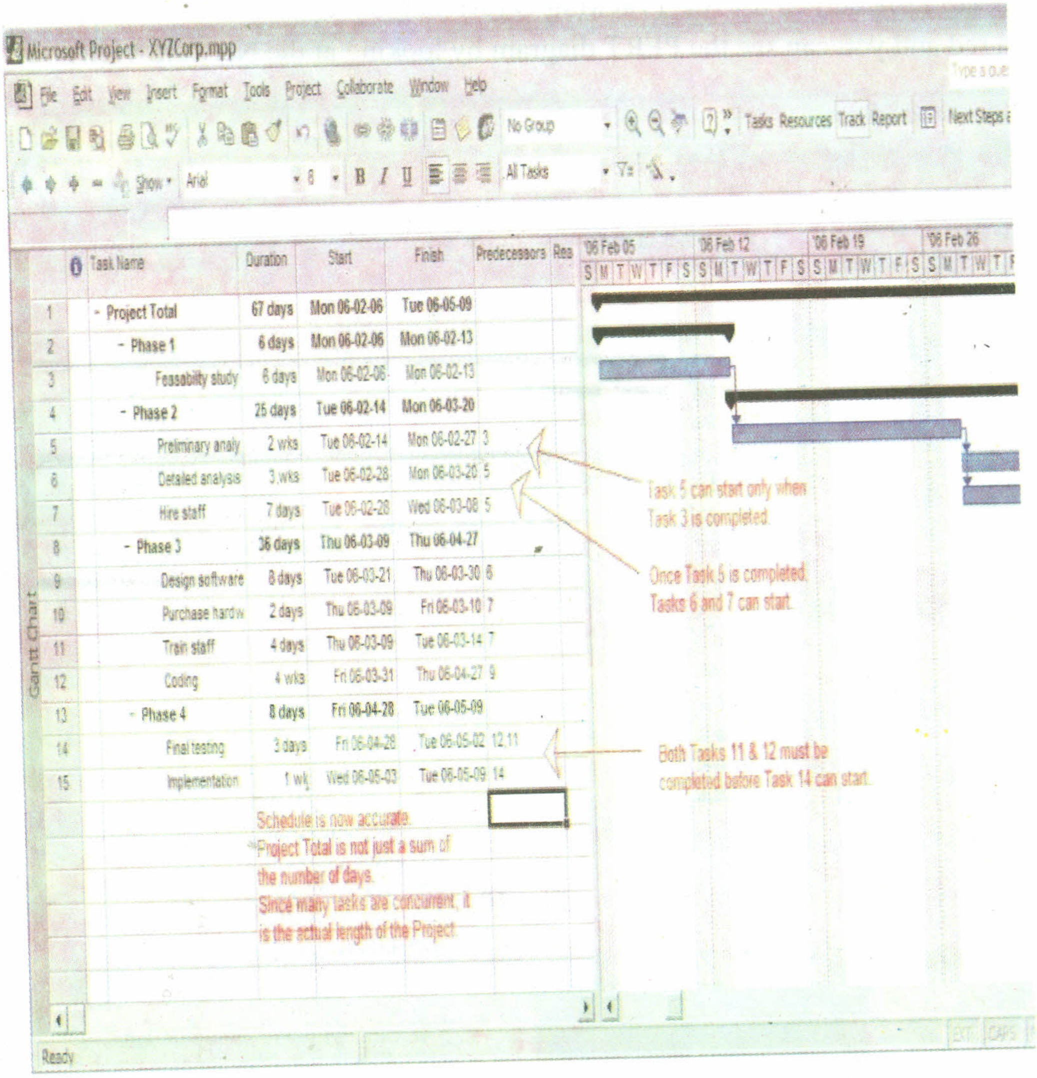


Fig. 9

3.5.3 Tracking Progress of the Project

Two of those techniques were called **Critical Path Management (CPM)** and **Program Evaluation and Review Techniques (PERT)**.

They were similar and you will now often find the technique referred to as: CPM/PERT.

The technique involves using network models to trace the links between tasks and to identify the tasks which are critical to meeting the deadlines.

When you have a large number of tasks overlapping you really have to use the right tool to show which tasks can be delayed and which must be on time.

Once you've identified the **critical path**, any delay on any part of the critical path will cause a delay in the whole project. It is where managers must concentrate their efforts.

In MS Project, you use the **Tracking Gantt** diagram to show the critical path in red and you can see the PERT diagram by looking at the Network view.

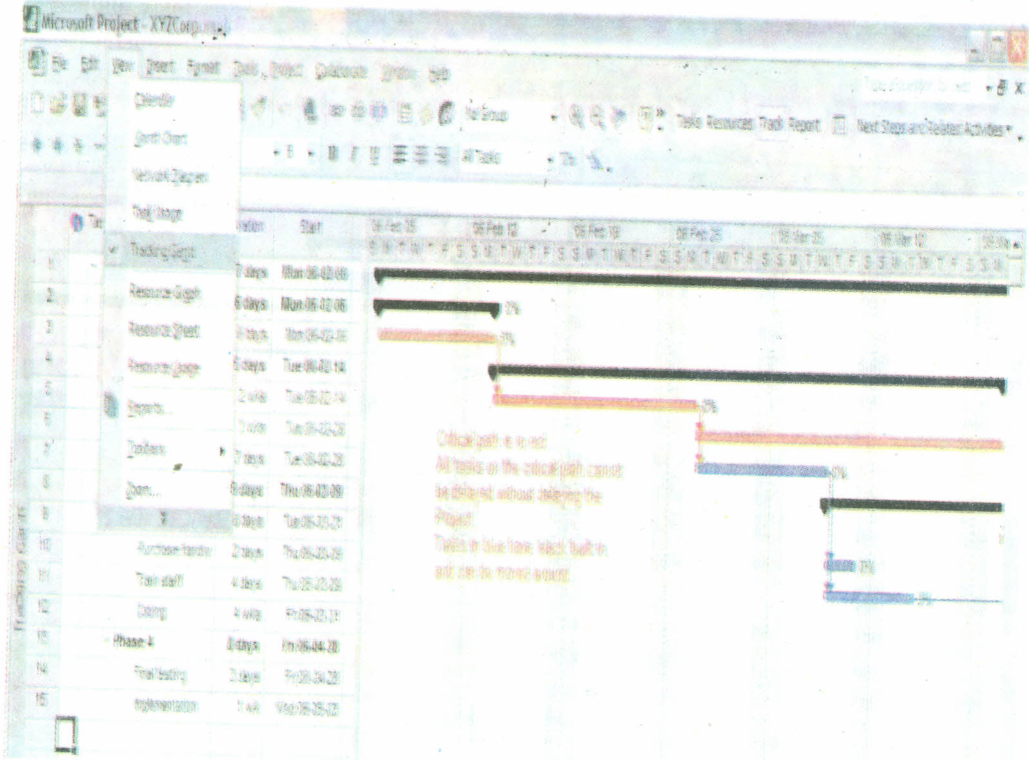


Fig. 10

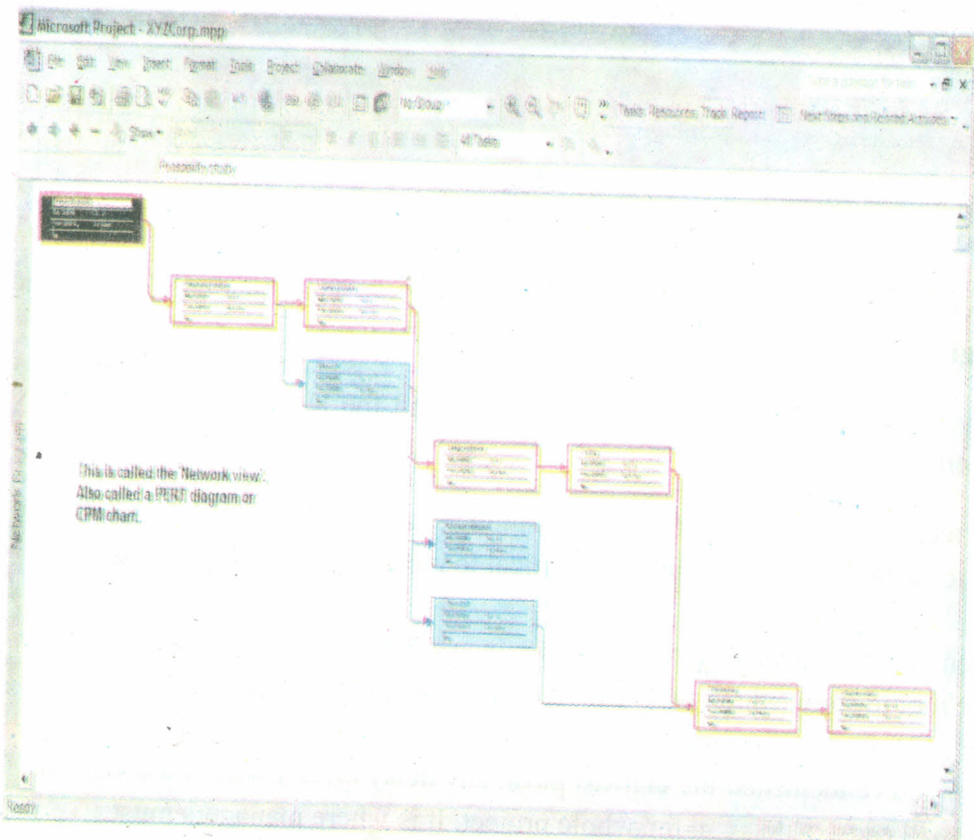


Fig. 11

Finally for this section, you'll want to track the degree of completion of each of the tasks.

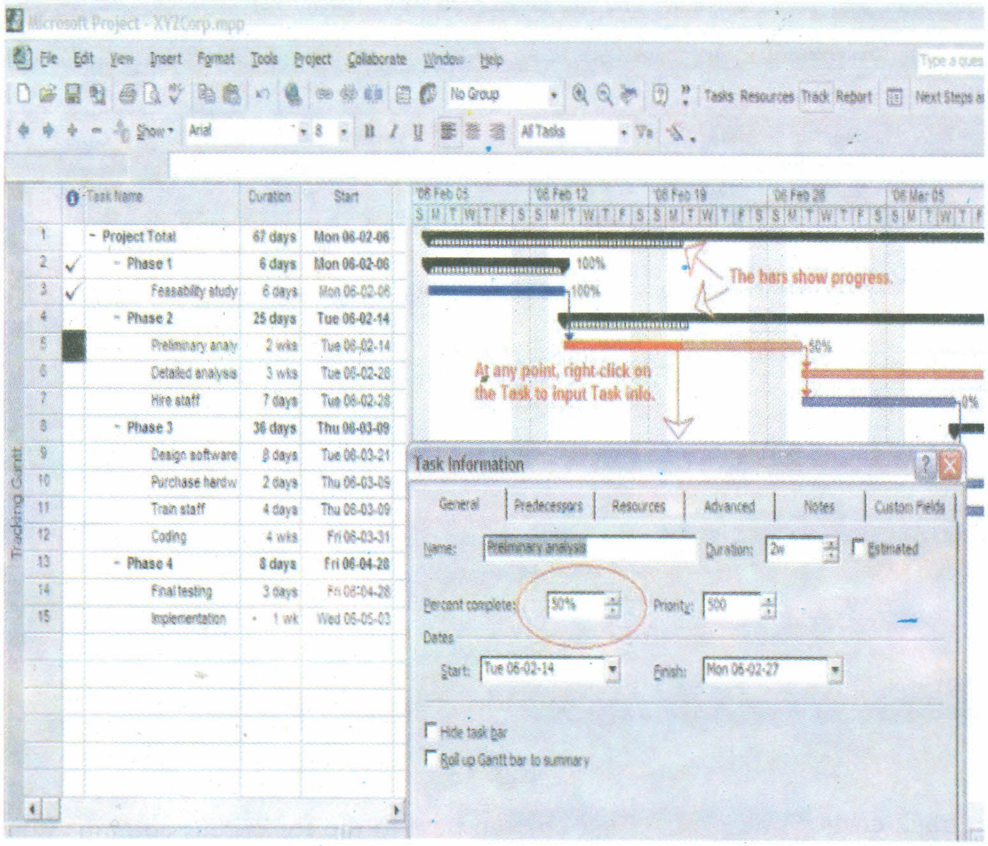


Fig. 12

3.5.4 Managing the Project Resources

You will need people to accomplish all those tasks that you've identified in the previous section. Those people are resources that you have to manage well in order to achieve the **project's objectives**.

You may also need some material resources - equipment, supplies, specialized environments - that you will have to schedule and pay for.

You can easily include the management of resources in **MS Project** along with the tasks because, after all, the resources are essential to the accomplishment of the tasks in the first place.

You must start by identifying the resources available along with their costs. Resource costs will be multiplied by duration to calculate project costs.

You have to open the Resource sheet to specify the project resources and costs.

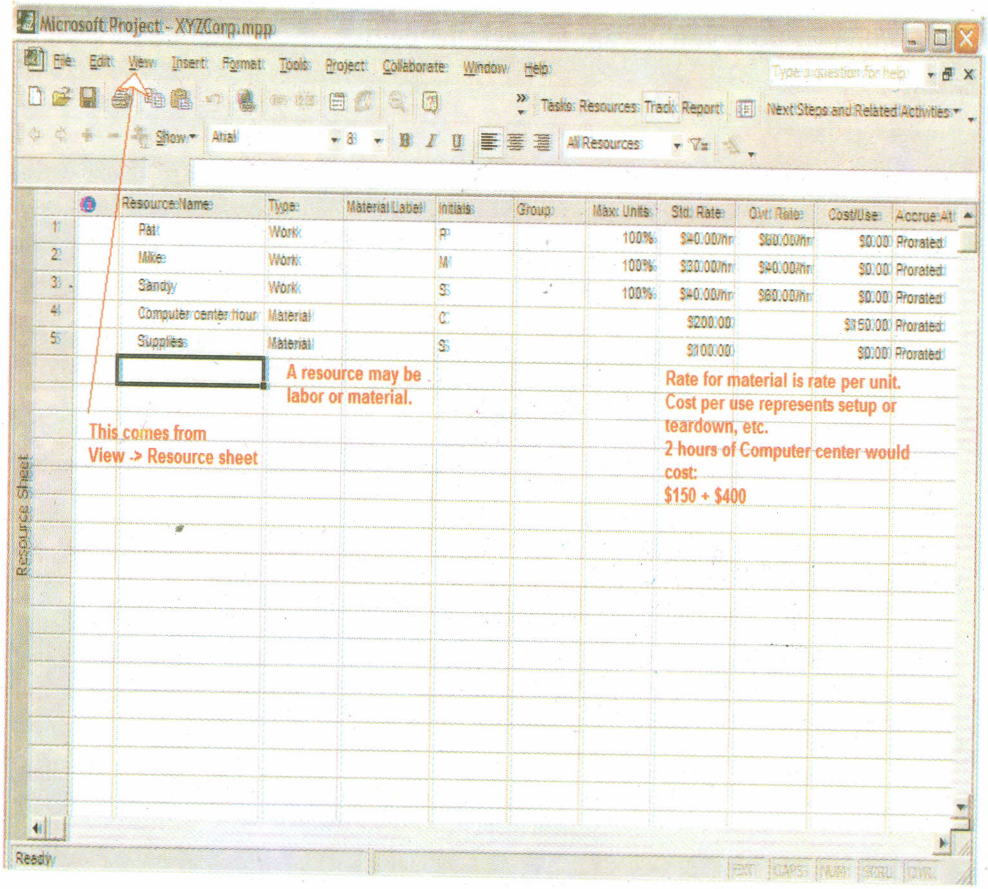


Fig. 13

To track costs, you insert a **Cost** column next to the Resources column. When you assign the resources to each task, the costs will be calculated and displayed.

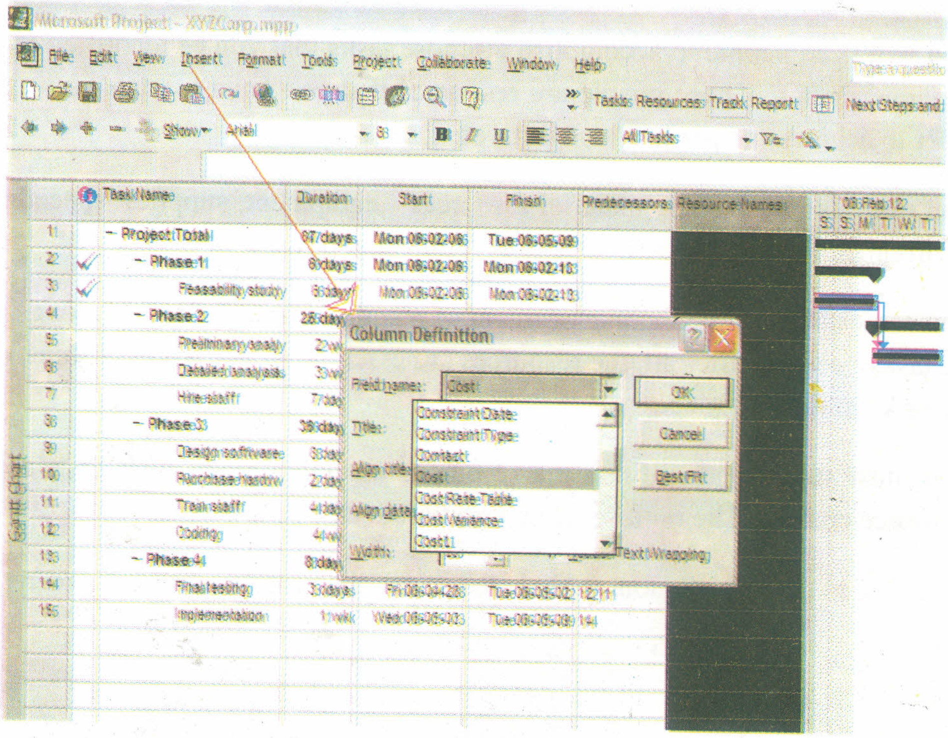


Fig. 14

You assign resources, people or material, to each of the tasks. A task may have several resources.

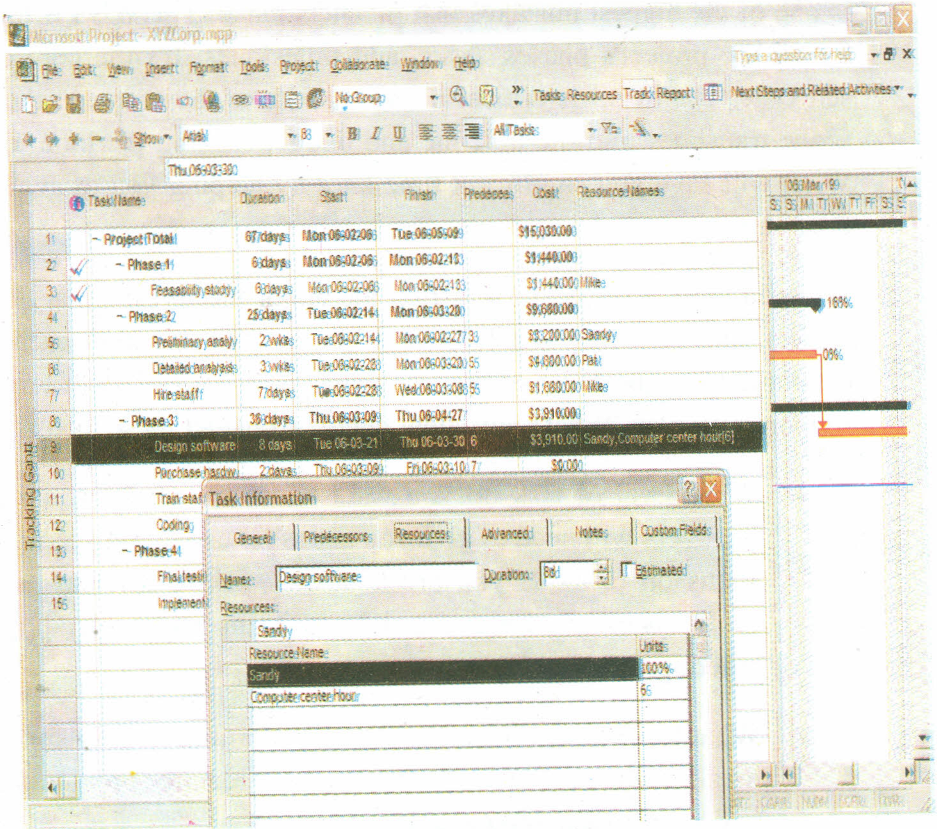


Fig. 15

3.6 STEP BY STEP PROCESS

Use the five-step process to make sure you don't go down the wrong path. Here we are assuming that you have already defined the project start date, applied the appropriate base calendar, and set up the default task type and other settings in the **Options** dialog box (**Tools** menu). If you haven't done so, see the related links in the **See Also** section of this page. Then perform the following five steps:

1. Create a task list and work breakdown structure (WBS)
2. Indent or out dent tasks to finalize the WBS
3. Enter task durations or work estimates
4. Create dependencies between tasks
5. Assign resources

You can do all of these tasks by using the default view. There are three types of views: Charts or graphs, Sheets, and Forms. The Entry table, which is the default table for the Gantt Chart, is also perfect for this process. The following steps will tell you when to insert additional columns.

Step 1: Create a task list and work breakdown structure (WBS)

WBS: A hierarchical structure that is used to organize tasks for reporting schedules and tracking costs. With Project, you can represent the work breakdown structure by using task IDs or by assigning your own WBS code to each task.

Failing to understand the importance of the work breakdown structure (WBS) is one of the biggest mistakes that planners make. The WBS is the hierarchical list of the project's phases, tasks, and milestones. It's the core of the project schedule. The WBS is critical because it drives the scope of the project. The scope translates into the timeline and budget. Taking the time to map out the WBS will save you significant time later by helping you to avoid rework and false starts.

To build your WBS, start by listing the major pieces (summary tasks) of your project, and then map out the minor pieces (tasks) within each major piece. Continue to break down each piece until you have sufficient level of detail to support your plan. What's sufficient detail? Consider these factors:

- What level of task do you want to track and report status on? Team members will need to give you status on tasks, and you'll need to report status on them. If you break down work_to one-day tasks and your project is months long, you and your team will be spending a lot of time entering and tracking status.
- What level of detail gives you early warning about risks? You want to break down your tasks so that you can identify problems early enough to do something about them.
- Can you effectively identify dependencies between tasks? If work on one thing can't start until work on another is finished, you need each work item to be a separate task so that you can indicate that dependency.

To enter summary tasks:

1. On the **View** menu, click **Gantt Chart**.
2. In the **Task Name** field, type a descriptive name for the first major phase of work or deliverable.
3. Continue to type descriptive names for each major phase of work or deliverable until you have entered all of your project's summary tasks.

Strictly speaking you are not creating summary tasks yet, because a real summary task must contain subtasks below it. Think of these as your draft summary tasks that will be fully developed later.

To enter tasks:

1. Select the first row under a summary task or subtask.

2. On the **Insert** menu, click **New Task**, and then type the task name in the inserted row.

3. Select the next row.

4. Repeat steps 2 and 3 until you have entered all of the work needed to complete the summary task.

5. Repeat the preceding steps until you have detailed all the summary tasks and subtasks in the project.

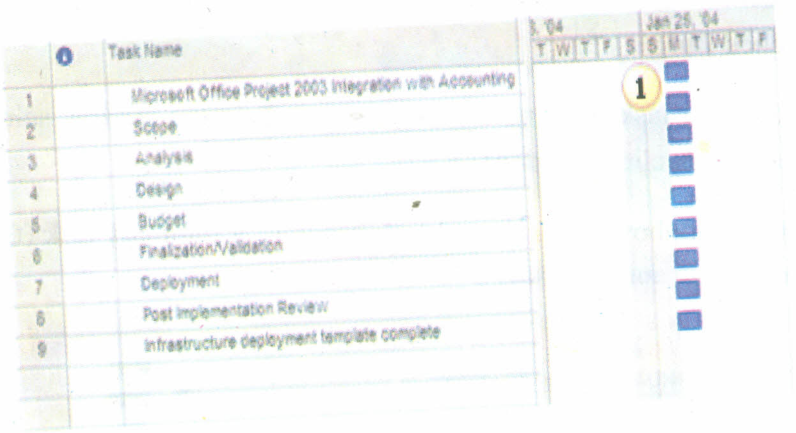


Fig. 16

When you enter new task names, Project automatically assigns them an initial duration of one day and schedules them to start at the project start date.

Duration: The total span of active working time that is required to complete a task. This is generally the amount of working time from the start to finish of a task, as defined by the project and resource calendar.

Be sure to also add milestones — markers of important completion points — at the end of each major activity to help measure progress and for benchmarking. It is a good practice to give milestone tasks a name that conveys completion or reaching an important point in the project lifecycle.

Step 2: Indent or outdent tasks to finalize the WBS

After you enter tasks in the **Task Name** field, it's time to create the hierarchy. You can stay in the **Task Name** field and use the **Indent** and **Outdent** buttons on the **Formatting** toolbar to establish the right outline levels. The key? Project differentiates between major phases of work, called summary tasks, and the smaller phases of work, called subtasks, based on indentation. Summary tasks have subtasks indented underneath them. Subtasks represent the actual work a resource will do, and they don't have additional subtasks indented under them.

Outline: A hierarchical structure for a project that shows how some tasks fit within broader groupings. In Project, subtasks are indented under summary tasks.

Usually when people talk about *tasks* in Project they're referring to subtasks, and when they talk about *phases* or *summary tasks* they're referring to summary tasks.

By using up to nine outline levels, you gain the ability to summarize data. Summary tasks consolidate information about the tasks below them. For instance, Project calculates the duration for summary tasks. A summary task's duration represents the total time it will take to complete the work for all of its subtasks. The project summary task summarizes the entire project.

Project summary task: A task that summarizes the duration, work, and costs of all tasks in a project. The project summary task appears at the top of the project, its ID number is 0, and it presents the project's timeline from start to finish.

To structure the task list

1. Click the task that you want to indent.
2. To indent a task, making it a subtask in the outline, select the task, and then click **Indent** .
3. To outdent a task, making it a summary task in the outline, select the task, and then click **Outdent** .

Notice how the task above the indented task becomes a summary task (the text and Gantt bar change automatically).

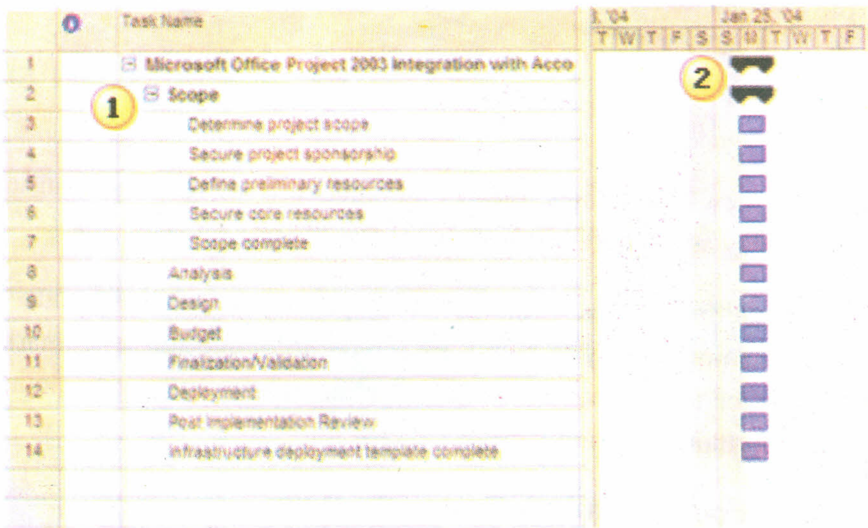


Fig. 17

In the figure:

1 Use the Indent and Outdent buttons to create the task hierarchy.

2 The Gantt bar for a summary task is formatted differently than that of subtasks.

You can highlight several tasks in a row and indent them all at once. Be sure to indent milestone tasks as well because they belong to the summary task. To quickly display the corresponding outline level numbers, on the **Tools** menu, click **Options**, click the **View** tab, and then select the **Show outline number** check box.

Here's an example of a complete outline, with outline numbers displayed.

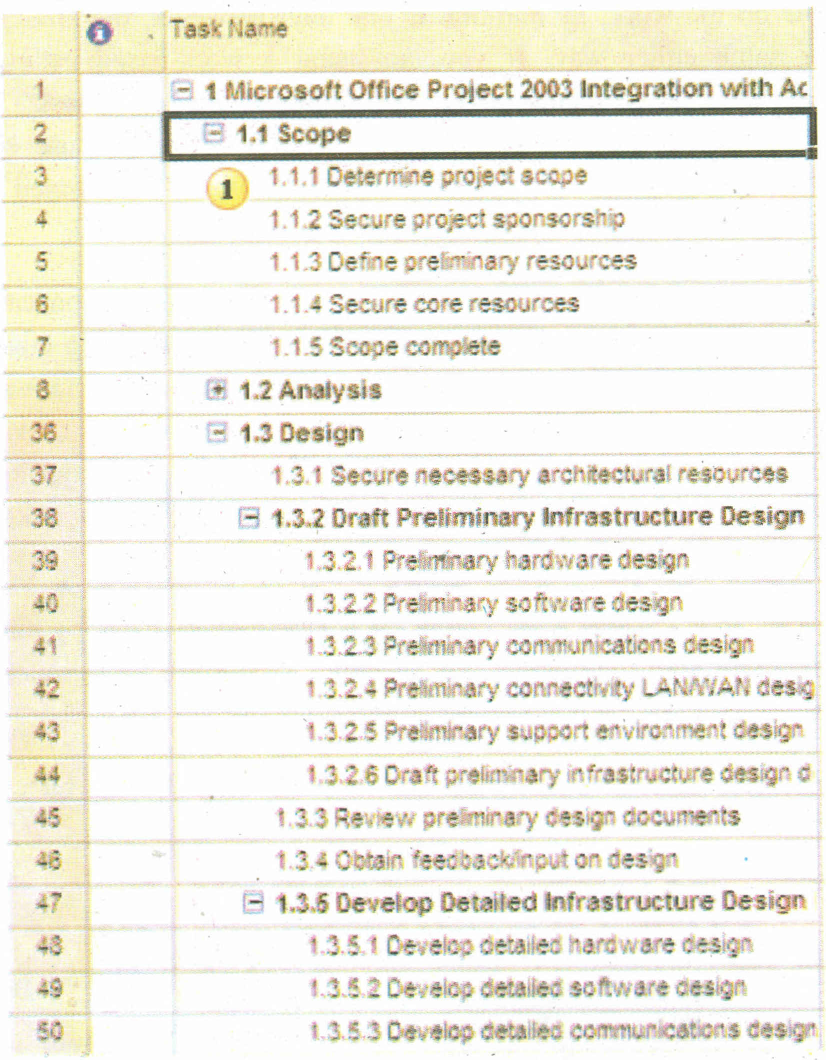


Fig. 18

In the figure:

(1) The outline numbers reflect the hierarchy or outline structure of the Project plan.

Project has the ability to display the outline as a Network Diagram, after the dependency structure has been established as described in the next step. Or you can use the Visio WBS Chart Wizard to view the outline in a more traditional chart or tree format. You can easily collapse and expand summary tasks to hide or show different levels of detail. Click **Expand** [+] or **Collapse** [−] beside a summary task to show or hide (respectively) its subtasks. You can also quickly show various outline levels by clicking **Show** on the **Formatting** toolbar.

Step 3: Enter task durations or work estimates

Effort-driven scheduling: The default method of scheduling in Project; the duration of a task shortens or lengthens as resources are added or removed from a task, while the amount of effort necessary to complete a task remains unchanged.

You can specify the time that you estimate it will take to complete the tasks by entering either work or duration. Work is the amount of effort or person hours needed to complete a task. Duration is the amount of actual time that will pass before the task is completed. Thus, if a task takes 16 hours of work and one person does the work, its duration is two days (assuming an 8-hour work day). If two people do the work, its duration is one day. However, the amount of work is the same either way. If you are using a work-based estimating approach, resource assignments drive the duration for each task. This scheduling approach is called effort-driven scheduling. You can use either method, but you should decide whether you want to use a work-based or a duration-based method of scheduling, and then stick with that method.

Entering work or duration is straightforward. Task work or duration can be entered directly in the **Work** or **Duration** field in any table or dialog box that displays those fields. It's important to understand that work and duration are measured in working days. For example, by default, 1 day = 8 hours, 5 days = 1 week, 20 days = 1 month. This means that if you type **30 days** in the **Duration** field, it is calculated as 6 weeks rather than a month. So make the correct conversions when entering values.

Note You can enter different time units on a task-by-task basis by simply typing the time unit after the number. For example, type **8min** for minutes, **8h** for hours, **8d** for days, **8w** for weeks, and **8mo** for months.

If most of your duration or work estimates will be weeks or months long, you can change the default time unit.

To change the default time unit for duration or work

1. On the **Tools** menu, click **Options**, and then click the **Schedule** tab.
2. In the **Duration is entered in** box, select the time unit you want.
3. In the **Work is entered in** box, select the time unit you want.
4. Click **Set as Default** to make the new settings the default in future projects.

When you enter work or duration in a plan, it is important to enter it at the subtask level because summary tasks are calculated fields. Project does not allow these values to be entered for a summary task.

To enter task durations:

1. On the **View** menu, click **Gantt Chart**.
2. In the **Duration** field of the task you want to change, type the duration you want.
3. Press ENTER.
4. Repeat the preceding steps for each task.

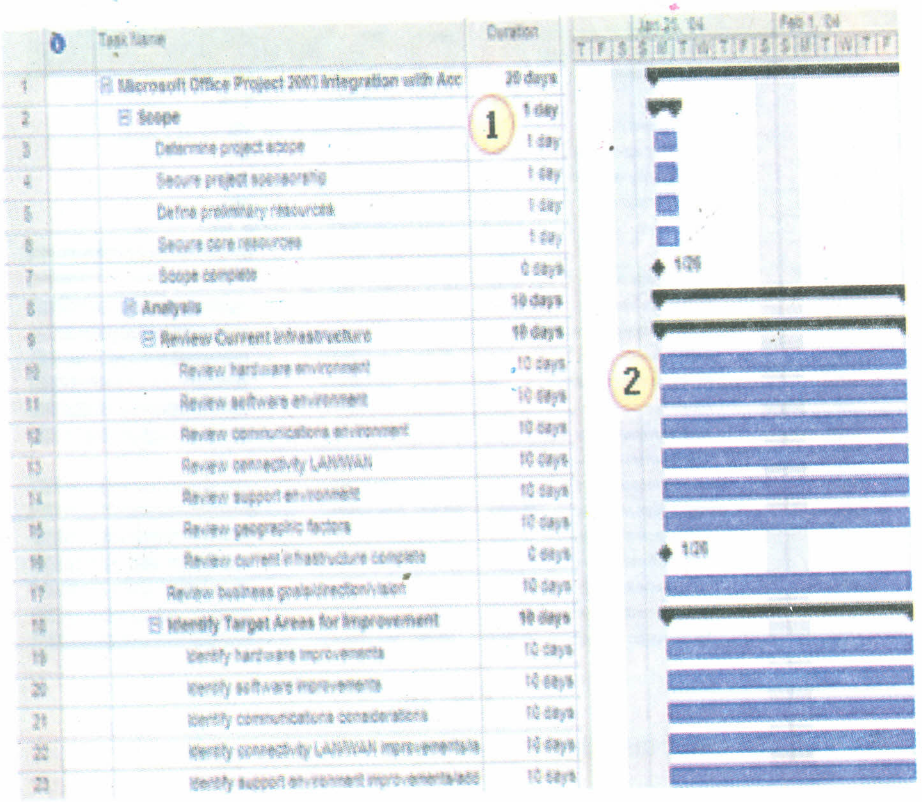


Fig. 19

In the figure:

① The durations of summary tasks span to include the earliest start and latest finish of their subtasks.

② As task durations change, Project redraws the task's Gantt bar to show the duration against a timeline.

You can change the duration of a task in many different views, tables, and dialog boxes in Project. If you change the duration in one place, it will change in every other location automatically. To mark a task as a milestone, type **0** in the **Duration** column.

If you are following a work-based scheduling approach, enter work estimates in the **Work** column. Note that if you choose this approach, durations will not be calculated until you complete step 5, which is assigning resources.

To enter work:

1. Click the **Start** column heading in the table portion of the Gantt Chart.
2. On the **Insert** menu, click **Column**.
3. Under **Field name**, select **Work**, and then click **OK**.
4. Type work estimates in the **Work** column for each task, just as you would type durations.

Fig. 20

1. You can enter task duration or work values, or both.
2. Note that a summary task's duration value shows the total amount of time it will take to complete the subtasks, while the summary task's work values show the total number of hours that will be spent working on the subtasks.

Step 4: Create dependencies between tasks

One of the most critical steps in scheduling is to create task dependencies, or links. This step makes the difference between a plan that can be used as an effective management tool and a plan that can only be used as a presentation tool.

A dependency occurs when the start or finish of one task depends upon the start or finish of another. Most tasks are dependent upon other tasks. After the dependencies are set, you can easily identify the critical path and understand the driving factors for the project end date. You can also easily make changes to one task and immediately see the ripple effect it will have on the rest of the plan. This is where Project shows its power as a tool for managing projects.

The challenge planners have is to ensure that all tasks are in the dependency chain. Here is a good rule of thumb: every task should have a predecessor unless it is driven by the start date of the project. Every task should have a successor unless it is the last task or milestone in the project.

When linking tasks, you can specify different types of dependencies. The most common dependency is Finish-to-Start (FS), which means that the predecessor task must finish before the successor task can start.

Linking: In a project, establishing a dependency between tasks. Linking tasks defines a dependency between their start and finish dates. In OLE, establishing a connection between programs so that data in one document is updated when it changes in another.

Critical path: The series of tasks that must be completed on schedule for a project to finish on schedule. Each task on the critical path is a critical task.

Predecessor: A task that must start or finish before another task can start or finish.

Successor: A task that cannot start or finish until another task starts or finishes.

There are many ways to set dependencies in Project:

To enter predecessor task IDs in the Task Form

1. On the **Window** menu, click **Split**.
2. Select the task that is dependent upon another.
3. In the **Task Form**, under the **Predecessor Name** box, select the task that this task is dependent upon.
4. Under **Type**, select **FS** (Finish-to-Start), **SS** (Start-to-Start), **FF** (Finish-to-Finish), or **SF** (Start-to-Finish).
5. Click **OK**.
6. To hide the Task Form, on the **Window** menu, click **Remove Split**.

To use the Link Tasks button

1. On the **View** menu, click **Gantt Chart**.
2. In the **Task Name** field, select two or more tasks you want to link in the order you want to link them.
   - To select nonadjacent tasks, hold down CTRL, and then click the tasks you want to link.
   - To select adjacent tasks, hold down SHIFT, and then click the first and last tasks you want to link.
3. Click **Link Tasks** .

To enter task IDs in the Predecessors column

1. If you can't see the Predecessor column, drag the split bar that appears between the Gantt Chart and the table to the right.
2. In the **Predecessors** field of the successor task, type the predecessor task's ID number and the appropriate dependency abbreviation: **SS**, **FF**, **FS**, or **SF**. If you don't specify a dependency type, Project applies a Finish-to-Start (FS) dependency.

As you set the dependencies, Project adjusts the schedule, even though you have not yet assigned your resources.

If two tasks need to overlap one another, or if they are dependent but there needs to be a gap between them, use the **Lag** field.

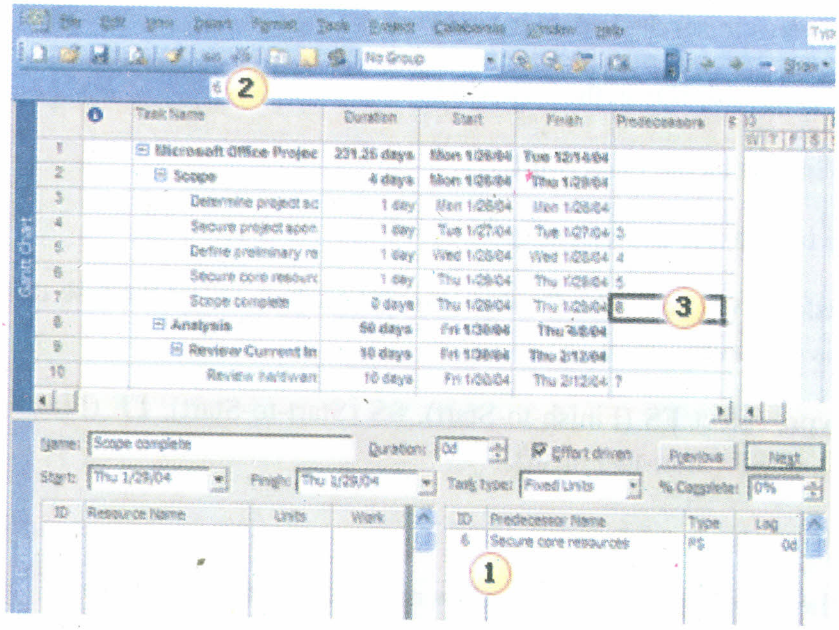


Fig. 21

1. One way to create task links is to enter predecessor task IDs in the Task Form.

2. Another way is to select two tasks, and then click the **Link Tasks** button.

3. Yet another way to link tasks is to enter task IDs in the **Predecessors** field.

Next, you might want to display your critical path, which identifies the path on which no slippage can occur without effecting the end date of the project.

To display the critical path

- On the **View** menu, click **Tracking Gantt**.

In this view, the Gantt bars of tasks on the critical path are formatted red.

If you want to further highlight the critical path, you can customize the view.

To format task names and Gantt bars of tasks on the critical path

1. On the **Format** menu, click **Gantt Chart Wizard**.
2. Click **Next**, select **Critical path**, and then click **Finish**.
3. Click **Format It**, and then click **Exit Wizard**.
4. On the **Format** menu, click **Text Styles**.
5. Under **Items to Change**, click **Critical Tasks**.
6. Under **Color**, click **Red**, and then click **OK**.

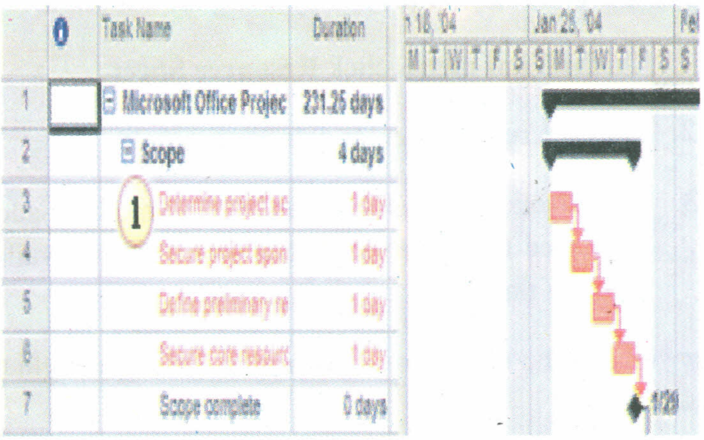


Fig. 22

1 This view is formatted to show tasks on the critical path with red task names and Gantt bars.

Step 5: Assign resources

How and which resources you want to assign depends upon your scheduling and tracking needs. There are three possible approaches:

- **Use Project to show responsibility for tasks.** This approach takes the least effort to enter and maintain. However, it does not give you any real insight into the status of work during the course of the project.

- **Use Project to forecast resource requirements.** This approach requires additional effort to enter and maintain assignments, and also requires assigning the correct work and unit values up front in the planning process. It provides more accurate information up front, but it does not provide information about the status of work during the project.

- **Use Project to forecast resource requirements and track what work resources actually do on tasks.** This approach requires the most effort because updates must be entered on tasks, but it also allows you to see how work on tasks is progressing during the course of the project.

Resources: The people, equipment, and material that are used to complete tasks in a project.

Generic resources: Placeholder resources that are used to specify the skills required for a specific task.

Make sure you understand what approach you need early on in the planning cycle to avoid significant rework of your plan. It is also important to determine what types of resources you need to assign. For example, you can assign named resources, such as Judy Lew, or generic resources such as Programmers. If you are early in the project-planning stage, you might want to use generic resources. Eventually, you will want to assign actual resources. You can also assign material resources such as computers, software, or other types of material (unit) costs.

After you understand what types of resources you need, you can add them to your project schedule.

To add resources to your project by using the Resource Sheet

1. On the **View** menu, click **Resource Sheet**.
2. For each resource, enter data in each field.
3. Double-click a resource name to modify additional data in the **Resource Information** dialog box, such as availability, cost rate, and working times.

After you add the resources to the project, you can begin to assign resources to tasks.

To assign resources by using the Resource Name field

1. On the **View** menu, click **Gantt Chart**.
2. If you can't see the **Resource Name** column, drag the split bar that appears between the Gantt Chart and the table to the right.
3. In the **Resource Names** field, select the resource that you want to assign to the task.
4. To assign multiple resources to the task, type a comma and repeat step 3.

To assign resources by using the Task Form

1. On the **Window** menu, click **Split**.
2. Select the task to which you want to assign resources.
3. In the **Task Form**, under **Resource Name**, click the resource that you want to assign.
4. To add another resource to the task, repeat step 3 in the next row of the **Resource Name** column.

To use resources by using the Assign Resources dialog box

1. On the **View** menu, click **Gantt Chart**.
2. On the **Tools** menu, click **Assign Resources**.
3. Select the tasks to which you want to assign resources.
4. Under **Resource from** in the **Assign Resources** dialog box, select the resources that you want to assign to the selected tasks.
5. Click **Assign**.

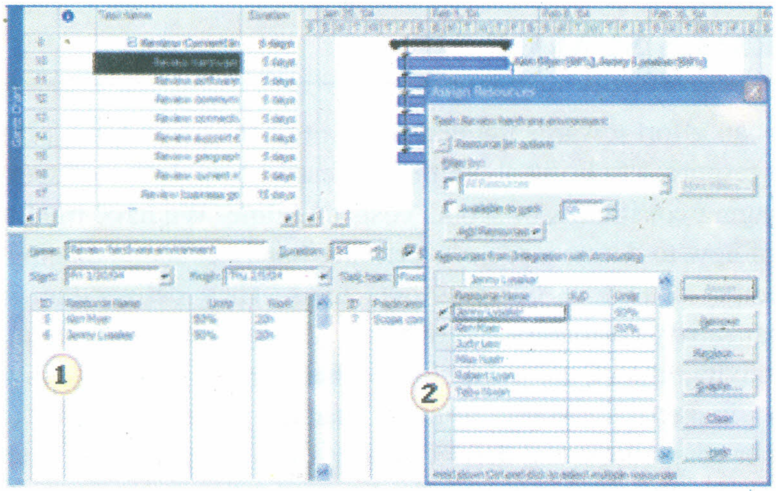


Fig. 23

1. Some ways to assign resources to tasks include selecting resource names from the **Resource Name** field or in the **Task Form**.

2. Another way to assign resources is to display the **Assign Resources** dialog box.

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 Project Management?

....

....

....

....

2) Explain the importance of Project Management.

....

....

....

....

3) Explain the term Template?

....

....

....

....

3.7 LET US SUM UP

This unit is an effort towards the management of the project, i.e. planning and organizing resources to bring about the successful completion of specific goals while managing constraints of scope, costs and time. We have tried to give an overview of how to define a project, defining timeline, and managing. Projects are the means to achieve business objectives. They deliver the goods and services that satisfy customers and owners. A project may be a large task or a complex activity, in fact, any work that is done to achieve an objective on time and within budget. The ability to better manage projects is a way to achieve the edge over competitors and deliver greater value to owners and customers. A template provides the basic framework of a project that was previously used in the system or from a project that was imported from MS-Project. A number of software tools are available in the market for project management like MS-Project, MS Visio etc.

3.8 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

1) It is the discipline of planning and organizing resources to bring about the successful completion of specific goals while managing constraints of scope, costs and time.
2) Projects are the means to achieve business objectives. They, along with ongoing operations represent the activities that make organizations run. They deliver the goods and services that satisfy customers and owners. A project may be a large task or a complex activity, in fact, any work that is done to achieve an objective on time and within budget. When you change the way people work, you are managing a project. More and more people recognize that their ability to effectively manage projects is now key to their success within the organization. The ability to better manage projects is a way to achieve the edge over competitors and deliver greater value to owners and customers.
3) A template provides the basic framework of a project that was previously used in the system or from a project that was imported from MS-Project. All fields and data are maintained when a project is saved as a template.

3.9 SUGGESTED READINGS

- http://office.microsoft.com/en-us/
- http://www.4pm.com/articles/projects.html
- http://www.rspa.com/
- Microsoft® Office Project 2007 Step by Step (Step By Step (Microsoft)) by Carl Chatfield and Timothy Johnson
- Microsoft Project 2007: The Missing Manual by Bonnie Biafore

UNIT 4 IMPLEMENTING CRISIS MANAGEMENT FRAMEWORK

Structure

4.0 Introduction
4.1 Objectives
4.2 Characteristics of a Crisis
4.3 Types of Crisis
4.4 Crisis Leadership
4.5 Stages of Crisis
- 4.5.1 Three-Stage Framework
- 4.5.2 Four-Stage Framework
- 4.5.3 Five-Stage Framework

4.6 Crisis Management Techniques
- 4.6.1 Establish a Crisis Management Team (CMT)
- 4.6.2 Develop a Crisis Response Plan
- 4.6.3 Update the Crisis Response Plan and Practice it Regularly
- 4.6.4 Establish a Strong Relationship with the Company's Legal Counsel
- 4.6.5 Putting it into Action

4.7 Models and Theories Associated with Crisis Management
- 4.7.1 Crisis Management Model
- 4.7.2 Management Crisis Planning
- 4.7.3 Contingency Planning
- 4.7.4 Business Continuity Planning
- 4.7.5 Structural-Functional System Theory
- 4.7.6 Diffusion of Innovation Theory
- 4.7.7 Role of Apologies in Crisis Management
- 4.7.8 Crisis Leadership
- 4.7.9 Unequal Human Capital Theory

4.8 Checklist for Crisis Management Planning
4.9 Examples of Successful Crisis Management
- 4.9.1 Tylenol (Johnson and Johnson)
- 4.9.2 Odwalla Foods
- 4.9.3 Mattel
- 4.9.4 Pepsi

4.10 Examples of Unsuccessful Crisis Management
- 4.10.1 Bhopal
- 4.10.2 Ford and Firestone Tire and Rubber Company
- 4.10.3 Exxon

4.11 Let Us Sum Up
4.12 Check your progress: The Key
4.13 Suggested Readings

4.0 INTRODUCTION

Unfortunate events occur in the life of most organizations that threatens to harm the organization, its stakeholders, or the general public.Such major events are referred as crisis. These crisis can be managed by trying to keep them from reoccurring and soften the impact of it when it does occur. The process by which an organization deals with crisis is called crisis management.

Crisis management is the organized attempt to avoid organizational crisis or to manage those crisis events that do occur. It mainly consists of skills and techniques required to assess, understand, and cope with crisis, especially from the moment it first occurs to the point that recovery procedures start. Crisis management contains methods that are required to respond to both the reality and perception of crisis such as a Crisis Management Plan. It also involves establishing metrics to define what scenarios constitute a crisis and should as a result trigger the essential response mechanisms. It also consists of the communication that occurs within the response phase of emergency management scenarios.

The credibility and reputation of organizations is greatly influenced by the perception of their responses during crisis situations. The organization and communication involved in responding to a crisis in a well-timed fashion makes for a challenge in businesses. There must be open and steady communication throughout the hierarchy to contribute to a effective crisis communication process.

A framework helps in understanding the field of crisis management and how one can better prepare for crisis events that may occur in the organization.

4.1 OBJECTIVES

After studying this unit, you should be able to:

- identify characteristics of a Crisis;
- list types of Crisis;
- understand Stages of Crisis;
- need of Crisis Management Techniques;
- explain Checklist for Crisis Management Planning; and
- list the examples of Successful Crisis Management.

4.2 CHARACTERISTICS OF A CRISIS

The various characteristic of a crisis are:

- **Unexpected**
  - Quick onset
  - Normal operating practices do not apply
  - Puts the organisation off-guard
- **Threat**
  - To health and life safety
  - To various business operations
  - To community, region, or globe
- **Quick response**
  - Communication may be tough
  - Information is incomplete, inaccurate or hard to obtain
  - Emotions are running high

4.3 TYPES OF CRISIS

There are many types of crisis but broadly it can be classified as:

1. Natural disaster
2. Technological crisis
3. Confrontation
4. Malevolence
5. Organizational Misdeeds
6. Workplace Violence
7. Rumours

- **Natural Crisis**

  Crisis that occur due to natural disasters which are considered as 'acts of God,' such as environmental phenomena as earthquakes, volcanic eruption, tornadoes and hurricanes, floods, landslides, tsunamis, storms, droughts that threaten life, property, and the environment itself are considered as natural crisis. For example: 2004 Indian Ocean earthquake (Tsunami)

- **Technological Crisis**

Crisis that are caused by human application of science and technology are known as technological crisis. When technology becomes complex and coupled and something goes wrong in the system as a whole is known as technological breakdown which leads to technological crisis. When human error causes disruptions is known as human breakdowns which results in some technological crisis. People tend to allocate blame for a technological disaster because technology is subject to human manipulation whereas they do not hold anyone responsible for natural disaster. The common type of technological crisis is software failures, industrial accidents, and oil spills. For example: Chernobyl disaster, Exxon Valdez oil spill.

- **Confrontation Crisis**

Those crisis which occur because of discontented individuals or groups who fight businesses, government, and various interest groups to win approval of their demands and expectations are called confrontation crisis. The most common type of confrontation crisis is boycotts, and other types are picketing, sit-ins, ultimatums to those in authority, blockade or occupation of buildings, and resisting or disobeying police. For example: Rainbow/PUSH's (People United to Serve Humanity) boycott of Nike.

- **Crisis of Malevolence**

This type of crisis occur when opponents or miscreant individuals use criminal means or other extreme tactics for the purpose of expressing hostility or anger toward, or seeking benefit from, a company, country, or economic system, perhaps with the goal of destabilizing or destroying it. The most type of this crisis is product tampering, kidnapping, malicious rumors, terrorism, and espionage. For example: 1982 Chicago Tylenol murders.

- **Crisis of Organizational Misdeeds**

The crisis that occur when management takes actions without adequate precautions that will harm or place stakeholders at risk. The different types of crisis of organizational misdeeds: crisis of skewed management values, crisis of deception, and crisis of management misconduct.

- **Crisis of Skewed Management Values**

These crisis are caused when managers favor short-term economic advantage and neglect broader social values and stakeholders other than investors. This state of lopsided values is rooted in the classical business creed that focuses on the benefits of stockholders and tends to view the benefits of its other stakeholders such as customers, employees, and the community. For example: Sears sacrifices customer trust.

- **Crisis of Deception**

  This crisis occurs when management hides or manipulates the information about itself and its products in its dealing with consumers and others. For example: Dow Corning's silicone-gel breast implant.

- **Crisis of Management Misconduct**

  The crisis that are caused not only because of skewed values and deception but also because of deliberate immorality and unlawfulness are known as crisis of management misconduct.

- **Workplace Violence**

  The crisis which occur when an employee or former employee commits violence against other employees on organizational grounds are known as workplace violence. For example: DuPont's Lycra.

- **Rumors**

  Wrong information about an organization cr its products creates crisis hurting the organization's reputation. The most common type of rumors is linking the organization to radical groups or stories that their products are contaminated. For example: Procter and Gamble's Logo controversy.

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 are the objectives of crisis management?

....

....

....

....

2) Why it is important to identify the types of crisis?

....

....

....

....

3) "Boycott" is an example of which type of crisis

....

....

....

....

4.4 CRISIS LEADERSHIP

Crisis due to situation charged emotionally, once becomes public leads to negative stakeholder reaction and thus has the potential to threaten the financial well-being, reputation, or survival of the organization. These crisis are categorized as organizational crisis. The two primary types of organizational crisis are:

1. Sudden crisis
2. Smoldering crisis

- **Sudden Crisis**

  Circumstances that occur without warning and beyond an institution's control are considered as sudden crisis. These crisis are the most often situations for which the institution and its leadership are not blamed.

- **Smoldering Crisis**

  Crisis that begin as minor internal issues like due to manager's negligence develops in to crisis status. These are situations when leaders are considered responsible for the crisis and its subsequent effect on the organization in concern.

4.5 STAGES OF CRISIS

By analyzing the stages of a crisis helped in accounting for a more holistic approach of understanding a crisis phenomenon. A three- or four-stage approach helps in analyzing the life of a crisis. A crisis is more than just an event. It is a life cycle phenomenon that has a birth, an acutest age, the crisis and an aftermath.

4.5.1 Three-Stage Framework

The most basic framework is the three-stage approach that includes a pre-crisis, crisis, and post-crisis format. This three-stage format is offered by Smith (1990). It consists of a pre-crisis period, the crisis of management; a crisis period, the operational crisis; and a post-crisis stage, the crisis of legitimation.

The **crisis of management** stage includes the actions of organizational leaders and a culture that does not put a premium on preparedness and can lead to a climate where all that is needed is a trigger event in order to start the crisis. In the **operational crisis** stage the organization should manage the crisis as best it can once it is under its way. This stage consists of building a supportive climate among the key players involved in the crisis. Unluckily, the **crisis of legitimation** stage may be characterized as scapegoating on the part of a number of parties including the organization itself as well as the government and the media. After a crisis occurs the organisation should appear legitimate in the eyes of the public.

Richardson (1994) also offered a three-step framework similar to the one proposed by Smith. The **pre-crisis/disaster phase** addresses the threats that can cause a crisis and also focuses on its prevention. The **crisis impact/rescue** stage is the occurrence of the actual crisis. In this period, management should work at mitigating the crisis and offering help to those affected by it. The **recovery/demise** stage focuses on restoring stakeholder confidence in the organization.

4.5.2 Four-Stage Framework

These frameworks offer more precision in examining the crisis progression. A four-stage approach was offered by Myers (1993) that begins with the **normal operations** stage in which prevention practices are established. During this stage operations are normal but preparations are made to address an event should one occur. The second stage **emergency response** includes the first hours immediately after the onset of the crisis. **Interim processing** is the third stage which represents an intermediate phase where temporary procedures are established until normal operations can resume. **Restoration** is the final stage that focuses on the transition back to normal operations.

Fink (1996) also offered a four-stage framework which begins with the **prodromal** stage. This stage occurs before the full-blown crisis and is tied up with warning signs that a crisis may be imminent. The **acute crisis** stage comes next and is evidenced by the sudden arrival of the event. In this stage crisis is most visible by outsiders to the organization. The **chronic crisis** stage is less dramatic in appearance, but is still noteworthy since the organization is trying to mop up the lingering damages from the episode. The **resolution** stage is the final stage where the organization is returning to its pre-crisis existence.

4.5.3 Five-Stage Framework

Pearson and Mitroff's (1993) offered a five-stage framework that provides an even more comprehensive approach to understanding the stages of a crisis. These stages include:

- **Signal detection**: The occurrence or the possibility of a crisis always begins with some forms of warning. Signal detection is the stage that advances those warnings. It include: Sense-making: represents a try to create an order and make sense retrospectively of what occurs. Perspective-taking: the capability to consider another person's or group's point of view.Becoming expert at signal detection is a mindset as well as a skill that organizations need to hold.

- **Preparation/prevention**: This stage consists of the formation of crisis management teams and plans for attacking those crisis that had been foreshadowed in the signal detection stage.The objective is to prevent as many crisis as possible and effectively manage those that do occur.

- **Containment/damage limitation**: In this stage the actual management of the crisis occurs. The concern is to contain the crisis to the greatest level possible and to mitigate the event so that organizational and stakeholder damage is kept to a minimum. Crisis handlers work diligently in this stage in order to bring the crisis to an end as quickly as possible, to limit the negative publicity to the organization and move into the business recovery phase

- **Recovery**: When crisis occurs, organizations must be able to carry on with their business in the middle of the crisis while at the same time should also be planning for how it will recover from the damage the crisis caused.So attempts are made to resume activities as close to normal as possible. The recovery will often proceed in stages as well. Short-term recovery goals to get the system back on line so that a minimal acceptable level of service is achieved. Long-term recovery follows as operational activities are restored to there pre-crisis level. In some cases, in the recovery process improvements are made which brings the level of operations up to a higher level than before the crisis. For example a company that experiences fire in its production facilities. After the fire, the new facility that is built should be better equipped with new machinery and technology than what existed in the old facility.

- **Learning:** It involves activities of reflection where lessons are learned from the crisis. The stress is not on searching for scapegoats and displacing the blame onto other parties rather a response often encouraged in a litigious society. Maximum attention is dedicated on improving current operational problems and preventing future ones. To make this possible organizational decision makers adopt a learning orientation and use earlier experience to develop new routines and behaviors that finally change the way the organization operates. The best leaders identify this and are purposeful and skillful in finding the learning opportunities inherent in every crisis situation.

Frameworks for Crisis Management

3-Stage Framework General	3- Stage Framework Smith , 1990	3-Stage framework Richardson 1994	4-stage Framework Myers 1993	4-Stage Framework Fink 1996	5- Stage Framework Pearson and Mitroff 1993
Before the crisis	Crisis of management	Precrisis / disaster phase	Normal Operations	Prodromal Crisis Stage	Signal Detection
					Preparation / Prevention
During the Crisis	Operational Crisis	Crisis Impact / Rescue phase	Emergency Response	Acute Crisis Stage	Containment / Damage limitation
			Interim Processing	Chronic Crisis Stage	
After the crisis	Crisis of legitimation	Recovery / demise phase	Restoration	Crisis Resolution Stage	Recovery
					Learning

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 difference between sudden and smoldering crisis?

....

....

....

....

2) Why it is important to understand a crisis in terms of its different stages?

....

....

....

....

3) Name the different stages present in five-stage crisis management framework.

....

....

....

....

4) Explain the learning stage present in crisis management framework.

....

....

....

....

4.6 CRISIS MANAGEMENT TECHNIQUES

4.6.1 Establish a Crisis Management Team (CMT)

This team comprises of the decision-makers present in the organization, each representing a different background and area of expertise. They can be from the public relations department, management, personnel, security and any specialists that relate to the specific industry. This team should also select a leader and a spokesperson. Initially this spokesperson is the only person who should be made available to the media. Availability of the CEO should be done on a limited basis, and he/she should not be the main spokesperson. The team members should be creative with strong problem-solving skills. This team will make all the crucial decisions during the time of crisis and will be intimately involved in every detail.

4.6.2 Develop a Crisis Response Plan

One of the CMT main responsibilities is to design a crisis response plan. It should be developed with the supposition that a crisis is any event, revelation, allegation or set of situations that threatens the integrity, reputation, or survival of an individual or an institution. These plans will direct the organization's activities in dealing with the crisis. Key to the process of designing this plan is creating a set of "worst-case scenarios" in which the group lists all the probable crisis the company could face for example from the CEO resigning to allegations that the company's products kill people. Many of the situations in between the two extremes can be grouped together and will have almost same response processes. Based on each potential crisis, a specific crisis plan should be designed to outline the exact response needed. Each plan would need materials, such as official statements, outlines for press releases, fact sheets and backgrounders, which deal with the situation, should be prepared ahead of time. Also, it is necessary to speak with one voice, so internal and external messages should be crafted to follow to this important guideline.

4.6.3 Update the Crisis Response Plan and Practice It Regularly

Once the plan is developed, it should not be forgotten rather it should be updated regularly. As the circumstances change the plan must also change accordingly. A company should implement the plan only when it practices the plan regularly. Role-playing exercises and seminars helps in preparing the crisis team for the stress of a crisis situation. The media can be merciless, particularly to an ill-prepared spokesperson. So it is essential that this person is prepped before speaking to the media. The speech patterns, camera presence and poor body language can all affect the delivery of the message.

4.6.4 Establish A Strong Relationship With The Company's Legal Counsel

There is a natural split between the legal, financial and communications departments of a company during a crisis. Everyone has its own idea as each one has its own unique angle and these ideas often collide. Despite of their conflicting views, it is necessary that there is teamwork between these groups. Hence, it is sensible for the communicators to develop a relationship with both legal and financial decision-makers .Thereby permitting for all the interests that are to be represented and a compromise should be developed ahead of time.

4.6.5 Putting It into Action

A complete crisis response plan and its implementation is important for effectively dealing with a crisis. Companies find themselves under the vigilant glare of the public at the time of crisis and every decision they make gets minutely examined. The first hours following a crisis are crucial as during this time the public will form its own opinions. Despite of all future actions, these opinions are almost impossible to change. Thus operational response is required. This response saves lives, property and other assets. The skill to communicate is also important. It saves the business. The public opinions will be based on both of these elements. So at the time of crisis, companies should:

- Communicate early and often.
- Show concern and assure that the company is doing everything possible to improve the situation.
- Be honest and open.
- Be constant in the message.
- Monitor public opinion using new technology like chat rooms, message boards, discussion groups, surveys.
- Follow up with public outlook surveys and employee questionnaires to learn from mistakes.

Most of the crisis cannot be avoided but efficiently responding to the situation may limit the negative impact the company suffers.

4.7 MODELS AND THEORIES ASSOCIATED WITH CRISIS MANAGEMENT

4.7.1 Crisis Management Model

Fruitfully defusing a crisis requires an understanding of how to handle a crisis before it occurs. Gonzalez-Herrero and Pratt offered a four-phase crisis management model process. This process includes:

- Issues
- Planning-prevention
- The crisis
- Post-crisis.

4.7.2 Management Crisis Planning

No corporation wants to face a situation that causes a substantial disruption to their business, especially one that stimulates extensive media coverage. Public inquiry can result in a negative financial, political, legal and government impact. Crisis management planning deals with providing the best response to a crisis.

4.7.3 Contingency Planning

Contingency plans are prepared in advance in order to make sure that an organization is appropriately prepared for a crisis. Crisis management teams can review crisis plan by developing a simulated scenario to use as a drill. The plan should clearly specify that the only people to speak publicly about the crisis are the designated persons, such as the company spokesperson or crisis team members. After a crisis breaks, the first hours are the most crucial. So it is important to work with speed and efficiency and the plan should specify how quickly each function should be performed. Information used should be accurate while preparing to offer a statement externally as well as internally. Providing wrong or manipulated information has a possibility of backfire and will greatly worsen the situation. This plan should contain information and guidance that will help decision makers to consider not only the short-term consequences but also the long-term effects of every decision.

4.7.4 Business Continuity Planning

When a crisis causes a substantial disruption to an organization a business continuity plan can help in minimizing the disruption. First, the critical functions and processes that are essential to keep the organization running must be recognized. Then each critical function and process must have its own contingency plan in the event that one of the functions/processes stops or fails. Testing these contingency plans by reviewing the required actions in a simulation will allow for all involved to become more sensitive and aware of the chances of a crisis. As a result, the team members will act more quickly and effectively at the time of the onset of an actual crisis.

4.7.5 Structural-Functional Systems Theory

The information provided to an organization at the time of crisis is critical to effective crisis management. Structural-functional systems theory focuses on the intricacies of information networks and levels of command making up organizational communication. It detects the information flow in an organization as **networks** made up of members and **links.** In organizations information flow in patterns called networks.

4.7.6 Diffusion of Innovation Theory

Diffusion of Innovation Theory is applied to the sharing of information. It is developed by Everett Rogers. This theory defines how innovation is disseminated and communicated through certain channels over a period of time. When an individual communicates a new idea to one or several others then diffusion of innovation in communication occurs. At its most basic form, the process involves:

- an innovation
- an individual or other unit of adoption that has knowledge of or practice of using the innovation
- another individual or other unit that does not yet have knowledge of the innovation
- a communication channel connecting the two units

The means by which messages get from one individual to another is known as a communication channel.

4.7.7 Role of Apologies in Crisis Management

Apology makes it feasible for an organization for possible legal consequences. Compensation and sympathy are two less expensive policies that are as effective as an apology in shaping people's perceptions of the organization taking responsibility for the crisis as these policies directly focus on the victim's needs. On one hand sympathy response expresses concern for victims while on the other hand compensation offers victims something to offset the suffering.

4.7.8 Crisis Leadership

Crisis leadership helps in organizational restructuring during and after a crisis. It is done in following manner:

1. By building an environment of trust

2. By reforming the organization's mindset
3. By recognizing apparent and obscure vulnerabilities of the organization
4. By making wise and quick decisions as well as taking courageous action
5. By learning from crisis to effect change

Leadership action in crisis reflects the competency of an organization as the test of crisis shows how well the institution's leadership structure serves the organization's objectives and withstands crisis. Effective human resources should be developed as it is vital during building organizational capabilities through crisis management executive leadership.

4.7.9 Unequal Human Capital Theory

The organizational crisis can result from discrimination lawsuits. This theory is derived from economic theories of human and social capital concluding that minority employees get fewer organizational benefits than those with access to executive management. This can lead to negative stakeholder reaction, damage the company's reputation, and threaten the corporate survival.

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) List the crisis management techniques.

....

....

....

....

2) What a company should do at the time of onset of crisis?

....

....

....

....

3) What is the role of apology in crisis management?

....

....

....

....

4) Explain Management crisis planning.

....

....

....

....

4.8 CHECKLIST FOR CRISIS MANAGEMENT PLANNING

A crisis is anything that has the capability of impacting significantly an organization. Companies having crisis management plans are able to:

- Work efficiently with local emergency responders city, state and federal agencies in responding to events;
- Promptly take care of the needs of those affected;
- Support investigating agencies without jeopardizing the company's legal position;
- Form working relationships with media and selected officials that will help get the company's message to the public;
- Prepare for probable litigation and claims;
- Provide correct and timely information;
- Reduce the diversion of corporate executives;
- Contain financial exposure; and minimize the incident effect on the company's reputation

Crisis management has four objectives:

- Reduce the strain during the incident;
- Demonstrate the corporate commitment and expertise;
- Control the flow and the correctness of the information;
- Manage resources efficiently.

Major elements of effective management planning consist of the identification of a crisis management team an assessment of the most likely crisis scenarios, the designing of a crisis management plan document, periodic crisis training exercises, adherence to crisis communication guidelines and constant review and refinement of the plan.

Create a Crisis Management Team and Assess Potential Crisis

The CMT team can contain legal counsel, investigators, public relations personnel, investor relation's personnel, risk manager, financial personnel, marketing personnel, employee relation's personnel, and technical personnel.

Develop Crisis Management Team plans

The chief objective of any plan is to build up a flexible structure that is capable of responding to any type of crisis rapidly, decisively and in a coordinated manner. The CMT plan should establish relationships, responsibilities and continuity. It comprises of a notification system with a specific and up to date listing of recent contact information of the team members, chain of command, outside relevant agencies.

Establish Guidelines for Gathering Information and Internal Investigations

The CMT should be ready to initiate the investigation, determine the facts, potential liability and available defenses. The team should implement rules that promote the fact-finding process.

- Identify who has the power to initiate an investigation;
- Identify who will regulate the scope of the investigation;
- Identify an attorney or investigator that is qualified to head the investigation;
- Prepare a preliminary list of employees and management with knowledge about particular crisis risks;
- Prepare guidelines that establish an initial schedule for the investigation and identify the information needed; and
- Define which team member will evaluate the results and what will be done with them.

The team should make efforts to maximize protections provided by legally known privileges, including attorney-privilege, work-product immunity doctrine and self-evaluative privilege.

Provide Periodic Crisis Training Evaluation

By having training on managing a crisis will enable everyone in understanding his or her roles in the plan. This training helps in addressing legal issues before they occur; develop investigation procedures; identify systems and equipment needed during a crisis and develop good media relation's skills.

Develop Guidelines for Crisis Communications

Good communication is the most important part of any crisis management plan. Communication should lessen strain, demonstrate a corporate commitment to correct the problem and take control of the information flow. Crisis communications consists of communicating with a range of constitutes: the media, employees, neighbors, investors, regulators and lawmakers.

The single most important element of the crisis response is public relations. Design guidelines for elected spokesperson covering how to work with the media and community leaders. Templates should be prepared for communicating with various scenarios. Attorneys on the crisis management team should review media statements and suggest answers to protect against privilege waivers and potential admission that can be used in litigation.

4.9 EXAMPLES OF SUCCESSFUL CRISIS MANAGEMENT

4.9.1 Tylenol (Johnson and Johnson)

Crisis not always strike a company purely because of its own negligence or misadventure. At times such situations are created which cannot be blamed on the company but it takes a huge amount of blame if it makes mistakes in its response. One such example of how a company can get it right is that of Johnson and Johnson and its response to the Tylenol poisoning.

In 1982, a murderer added 65 milligrams of cyanide to some Tylenol capsules on store shelves. As a result seven people died including three in one family. The company recalled and destroyed 31 million capsules at a cost of $100 million. The affable CEO, James Burke, appeared in television ads and at news conferences informing consumers about the company's actions. Tamper-resistant packaging was quickly introduced and Tylenol sales speedily bounced back to near pre-crisis levels.

4.9.2 Odwalla Foods

Odwalla is the health-conscious juice company which was started a couple of decades ago when Greg Steltenpohl, Gerry Percy and Bonnie Bassett began squeezing fresh oranges on a $200 hand juicer. The company was rising strongly with annual sales rising 30% per year and approaching $90m. When Odwalla's apple juice was found to be the cause of an outbreak of E. coli infection, the company lost a third of its market value. In October 1996, an outbreak of E. coli bacteria in Washington State, California, Colorado and British Columbia was found to unpasteurized apple juice manufactured by natural juice maker Odwalla Inc. Forty-nine cases were stated, including the death of a small child. Within 24 hours, Odwalla discussed with the FDA and

Washington state health officials; made a schedule for daily press briefings; sent out press releases which declared the recall; expressed regret, concern and apology, and took responsibility for anyone harmed by there products; detailed symptoms of E. coli poisoning; and described what consumers should do with any affected products. With the help of consultants Odwalla then developed effective thermal processes that would not harm the products' flavors when the production restarted. All of these steps were conversed through close relations with the media and through full-page newspaper ads.

4.9.3 Mattel

The toy maker company, Mattle Inc. has been plagued with more than 28 product recalls. In summer of 2007 the company faced two product recall in two weeks due to the problems with exports from China. The company did all that it can do in order to get its message out and thereby earns high marks from consumers and retailers. Although they were upset by the condition but they appreciate the company's response. Just after the 7 a.m. recall announcement by federal officials at Mattle, public relations staff comprises of 16 was set to call reporters at the 40 biggest media outlets. They asked each to check their e-mail for a news release outlining the recalls, invited them to a teleconference call with executives and scheduled TV appearances or phone conversations with Mattel's chief executive. The Mattel CEO Robert Eckert had 14 TV interviews on Tuesday in August and about 20 calls with individual reporters. By the end of the week, Mattel had replied to more than 300 media inquiries in the U.S. alone.

4.9.4 Pepsi

A crisis in 1993 was faced by the Pepsi Corporation which started. It claims presence of syringes in cans of diet Pepsi. Pepsi advised stores not to remove the product from shelves till the situation is completely investigated. This led to an arrest. The company made this news public and then followed with their first video news release. This release shows the complete production process in order to demonstrate that such tampering was not possible within there factories. A second video news release exposed the man arrested. A third video news release showed surveillance from a store where a woman was caught replicating the tampering incident. The company at the same time publicly worked with the FDA during the crisis. The corporation was totally open with the public throughout, and every employee of Pepsi was kept aware of the details. This made public communications effective throughout the crisis. After the crisis was resolved, the corporation arranged a series of special campaigns so as to thank the public for standing by the corporation along with coupons for further compensation. This case showed a design for how to handle other crisis situations.

4.10 EXAMPLES OF UNSUCCESSFUL CRISIS MANAGEMENT

4.10.1 Bhopal

The Bhopal disaster is one in which poor communication before, during, and after the crisis cost thousands of lives. This incident illustrates the importance of incorporating cross-cultural communication in crisis management plans. The local residents were not aware as to how to react to warnings of potential threats from the Union Carbide plant. Operating manuals were printed only in English. This is an extreme example of mismanagement as well as indicative of systemic barriers to information distribution. According to Union Carbide's own chronology of the incident (2006), a day after the crisis Union Carbide's upper management reached India but was unable to support in the relief efforts because they were placed under house arrest by the Indian government. Symbolic intervention can be counterproductive; a crisis management policy can help upper management in making more calculated decisions in how they should react to disaster scenarios. The Bhopal incident illustrates the trouble in constantly applying management standards to multi-national operations and the blame shifting that often results from the lack of a clear management plan.

4.10.2 Ford and Firestone Tire and Rubber Company

The Ford and Firestone Tire and Rubber Company quarrel become known in August 2000. In response to claims that their 15-inch Wilderness AT, radial ATX and ATX II tire treads were separating from the tire core leads to horrible, spectacular crashes Bridgestone/Firestone recalled 6.5 million tires. These tires were commonly used on the Ford Explorer, the world's top-selling sport utility vehicle (SUV).

The two companies committed three major blunders on the onset of the crisis. First, they accused consumers for not inflating their tires correctly. Then they accused each other for faulty tires and faulty vehicle design. Last, when they were called to Washington to testify before Congress then they said very little about what they were doing to solve the problem that had caused more than 100 deaths.

4.10.3 Exxon

On March 24, 1989, a tanker belonging to the Exxon Corporation ran aground in the Prince William Sound in Alaska. The Exxon Valdez leaked millions of gallons of crude oil into the waters off Valdez. This results in killing of thousands of fish, fowl, and sea otters. Hundreds of miles of coastline was polluted. Numerous fishermen, mainly Native Americans, lost their livelihoods. On the contrary Exxon did not react speedily in terms of dealing with the media and the public. The CEO, Lawrence Rawl did not become an active part of the public relations work and actually avoided public involvement. The company had neither a communication plan nor a communication team in place to handle the event. The company did not assign any public relations manager to its management team until 1993, 4 years after the incident. Exxon established its media center in Valdez, a location too small and too far to handle the onslaught of media attention and the company acted protectively in its response to its publics, even laying blame, at times, on other groups such as the Coast Guard. These responses also happened within the days of the incident.

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 is the advantage of having crisis management plan?

....

....

....

....

2) What are the major elements of effective management planning?

....

....

....

....

3) Give two example of successful and unsuccessful crisis management.

....

....

....

....

4.11 LET US SUM UP

The field of crisis management is rising in scope and sophistication. Such changes should be acknowledged by recognizing that crisis management should be apart of the strategic management process. A crisis management framework should be designed that recognizes the various phases of the crisis management process. A framework is important because it guides us through the process of crisis management in a systematic manner that is both reactive and proactive. By reactive, it means responding to the crisis event efficiently with a minimal amount of damage. By proactive, it means planning for such events before they occur, and learning from these events after they have become known.

4.12 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

1) The objectives of crisis are:

   - Reduce the strain during the incident:
   - Demonstrate corporate commitment and expertise;
   - Control the flow and the correctness of the information;
   - Manage resources efficiently.

2) As different crisis necessitate the use of different crisis management strategies therefore it is important to identify the types of crisis.

3) "Boycott" is an example of confrontation crisis.

Check Your Progress 2

1) Smoldering crisis differ from sudden crisis in that they begin as minor internal issues like due to manager's negligence develops to crisis status.

2) By analyzing the stages of a crisis helped in accounting for a more holistic approach of understanding a crisis phenomenon.

3) The different stages present in five-stage framework are:

   - Signal detection;
   - Preparation and prevention;
   - Containment and damage control;
   - Business recovery;
   - Learning.

4) Learning stage involves activities of reflection where lessons are learned from the crisis. The stress is not on searching for scapegoats and displacing the blame onto other parties rather a response often encouraged in a litigious society. Maximum attention is dedicated on improving current operational problems and preventing future ones. To make this possible organizational decision makers adopt a learning orientation and use earlier experience to develop new routines and behaviors that finally change the way the organization operates. The best leaders identify this and are

purposeful and skillful in finding the learning opportunities inherent in every crisis situation.

Check Your Progress 3

1) The Crisis Management Techniques are:

- Establish a Crisis Management Team
- Develop a Crisis Response Plan
- Update the Crisis Response Plan and Practice It Regularly
- Establish a Strong Relationship with the Company's Legal Counsel
- Putting It into Action

2) At the time of onset of crisis a company should:

- Communicate early and often.
- Show concern and assure that the company is doing everything possible to improve the situation.
- Be honest and open.
- Be constant in the message.
- Monitor public opinion using new technology like chat rooms, message boards, discussion groups, surveys.
- Follow up with public outlook surveys and employee questionnaires to learn from mistakes.

3) The role of apology in crisis management is that it makes it feasible for an organization for possible legal consequences.

4) Management Crisis Planning:

No corporation wants to face a situation that causes a substantial disruption to their business, especially one that stimulates extensive media coverage. Public inquiry can result in a negative financial, political, legal and government impact. Crisis management planning deals with providing the best response to a crisis.

Check Your Progress 4

1) Companies having crisis management plans are able to:-

- Work efficiently with local emergency responders city, state and federal agencies in responding to events;
- Promptly take care of the needs of those affected;

- Support investigating agencies without jeopardizing the company's legal position;
- Form working relationships with media and selected officials that will help get the company's message to the public;
- Prepare for probable litigation and claims;
- Provide correct and timely information;
- Reduce the diversion of corporate executives;
- Contain financial exposure; and minimize the incident effect on the company's reputation

2) Major elements of effective management planning consist of the identification of a crisis management team an assessment of the most likely crisis scenarios, the designing of a crisis management plan document, periodic crisis training exercises, adherence to crisis communication guidelines and constant review and refinement of the plan.

3) Pepsi and Mattel are example of successful crisis management and Bhopal and Exxon are examples of unsuccessful crisis management.

4.13 SUGGESTED READINGS

- Barton, L. (2007). *Crisis leadership now: A real-world guide to preparing for threats, disaster, sabotage, and scandal*. New York, NY: McGraw-Hill.
- Coombs, W. (2007). *Ongoing crisis communication:Planning, managing, and responding* (2nd ed.).Thousand Oaks, CA: Sage.
- Dezenhall, E.; Weber, J. (2007). *Damage control: Why everything you know about crisis management is wrong*. Portfolio Hardcover
- Fink, S. (2007). *Crisis management: Planning for the inevitable*. Backinprint.com.
- Ulmer, R. R.; Sellnow, T. L., & Seeger, M. W. (2006). *Effective crisis communication: Moving from crisis to opportunity*. Thousand Oaks, CA: Sage Publications

NOTE

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

ISBN-978-81-266-7515-5