ignou
THE PEOPLE'S
UNIVERSITY

Indira Gandhi National Open University
School of Vocational Education and Training

MSEI-026
BCP, DR PLANNING
AUDIT

BCM Program Management

4

''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

4

BCM PROGRAM MANAGEMENT

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	Mr. Jitender Sethi	Mr. Hemant Parida
Dy. Registrar (Pub.)	Asstt. Registrar (Pub.)	Proof Reader
MPDD, IGNOU	MPDD, IGNOU	MPDD, IGNOU

November, 2011

ISBN: 978-81-266-5716-2

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 BCM Program Management. Ensuring applications and data are available during planned and unplanned outages is called as Continuity. Today, Business Continuity Management (BCM) is a standard management process in many large organizations, and governments across the world. BCM is an important process for the organizations for their economies implement. The Maintenance and administering process of BCM is very patchy, and many organizations that claim to have implemented BCM do not ensure that their business continuity capability is either up to date or effective. BCM covers disaster recovery, crises management, risk management controls and Technology recovery. It explores the approach of Business Continuity in case of a Disaster, with minimum resources, and maximum output. Every department either IT or Production BCM applies equally on Management and Operational staff as well as Technology and geographical location. 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 maintaining and administering BCM Plans. BCM is an iterative process, and needs to be actively managed. The initial aim of the stages will be to successfully complete an implementation of the BCM Lifecycle, the long term goal of BCM programme management is to improve the organization's BCM capability, and hence its operational resilience, with successive iterations of the BCM Lifecycle.

The **Unit two** provides an overview of the auditing and evaluating BCM plans. BCM is an important risk management program designed to protect companies from potential significant consequences related to events that can disrupt critical business processes. The auditing and evaluating of BCM program can help the organization understand the risks and the options to create an effective BCM program. Managers throughout the organization must be held accountable for appropriately managing the risks associated with disruption of the business operations and associated functions within their organization.

The **Unit three** covers developing and implementing a BCM response which includes developing and implementing crisis response actions for responding to and stabilizing the situation following an incident or event, establishing and running an Emergency Operations Center to be used as a command center during the crisis, practical experience in handling incidents/emergencies and designing, developing and implementing plans that provide continuity within recovery time and/or recovery point objectives.

The **Unit four** covers disaster simulation exercise. Disasters have resulted in significant morbidity, mortality and economic loss. Now better plans are now available for effective disaster management as well as for the reduction of preventable losses.

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 MAINTAINING AND ADMINISTERING BCM PLANS

Structure

1.0 INTRODUCTION

Ensuring applications and data are available during planned and unplanned outages is called as Continuity. Today, Business Continuity Management (BCM) is a standard management process in many large organizations, and governments across the world. BCM is an important process for the organizations for their economies implement. The Maintenance and administering process of BCM is very patchy, and many organizations that claim to have implemented BCM do not ensure that their business continuity capability is either up to date or effective.

BCM covers disaster recovery, crises management, risk management controls and Technology recovery. It explores the approach of Business Continuity in case of a Disaster, with minimum resources, and maximum output. Every

department either IT or Production BCM applies equally on Management and Operational staff as well as Technology and geographical location.

Businesses with dependency of Information technology are most vulnerable victim of any disaster. Starting from Data entry to month end posting, each operation is dependable on various process including technology and human interference. Hardware using OS, carrying Databases, running applications, entering data, collecting documents are dependable operations, of each other. One layer disturbance can hold the operations with in no time.

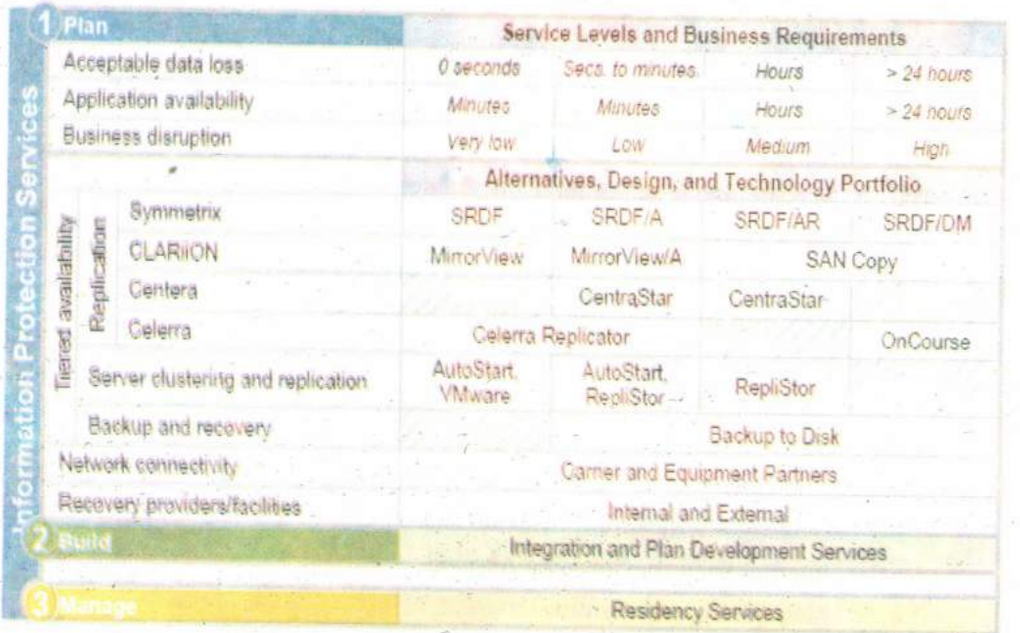

Fig. 1: Business Continuity Framework

1.1 OBJECTIVES

After studying this unit, you should be able to:

- know that organization proactively prepared and respond to unplanned events;
- asses that the business possesses the BCM plan it needs to react to man-made or natural disruptive events;
- protect the organization in DR;
- assess the risks;
- develop a tailored business resilience strategy;
- safeguard business-critical information while maintaining continuous operations;
- enable a virtually complete recovery; and
- maintain and administering BCM plan using IT tools.

1.2 BUSINESS CONTINUITY REQUIREMENTS

Business Continuity Management (BCM) is a company-wide approach designed to ensure that critical business functions can be maintained or restored as quickly as possible in the event of internal or external incidents. One of the aims of BCM is therefore to minimize the financial, legal and reputational impact of such incidents.

Overall, BCM is intended to ensure the continuation or rapid recovery of business activity in crisis situations. A Business Impact Analysis is carried out to identify business critical resources and processes; this will include defining appropriate recovery times and availabilities. The Business Continuity Strategy forms the basis for the Business Continuity Plans. These define (in the sense of preparatory measures, checklists and work tools) the procedure for the timely and correct recovery of business activity. The Business Continuity Strategy can be an integral component of an institution's corporate strategy. The strategy must provide explicit information on any specific residual risks that are consciously accepted. The development and implementation of a BCM process will focus in particular on the following areas:

- Definition including scope of BCM
- Anchoring of BCM in the corporate organisation
- Definition of crisis scenarios and their impact on the company's resources
- Identification of business-critical resources and processes together with an analysis of the impact of losing them by means of a Business Impact Analysis (BIA)
- Definition of the Business Continuity Strategy for the fundamental approach to dealing with losses of individual business architecture resources
- Preparation of Business Continuity Plans designed to permit the recovery of business-critical processes and resources in a crisis situation
- Business Continuity Reviews and Business Continuity Tests for the Business Continuity Plans and crisis management organisation
- Reporting, communication and training.
- Continuous availability / operational resilience
- Keep business running around the clock, around the world
- Keep business running through disasters and maintenance cycles

- Operational recovery / application availability
- Keep minor operational issues from affecting productivity
- Keep business applications up and running

Why Focus on Availability and Recovery? Substantial Number of Outages Due to Failures and Disasters can be shown as under -

a. Continuous availability through disasters (<1% of occurrences)
   - Flood, fire, earthquake
   - Contaminated building

b. Operational recovery from failures (13% of occurrences)
   - Database corruption
   - Component failure
   - Human error

c. Availability through planned outages due to competing workloads (87% of occurrences)
   - Backup, reporting
   - Data-warehouse extracts

Achieving Business Continuity

Determine requirements / service levels

- System / application mapping

Validate ability to achieve service-level agreements

- Evaluate costs / tradeoffs of technologies to meet service levels

Create right level of protection for the specific business and application requirements

Tie it all together

- Across storage platforms
- Across infrastructure (storage, servers, networks, applications)
- Across data centers and geographic locations
- Simplify management overhead and implementation risk by working with vendors who can manage the whole project

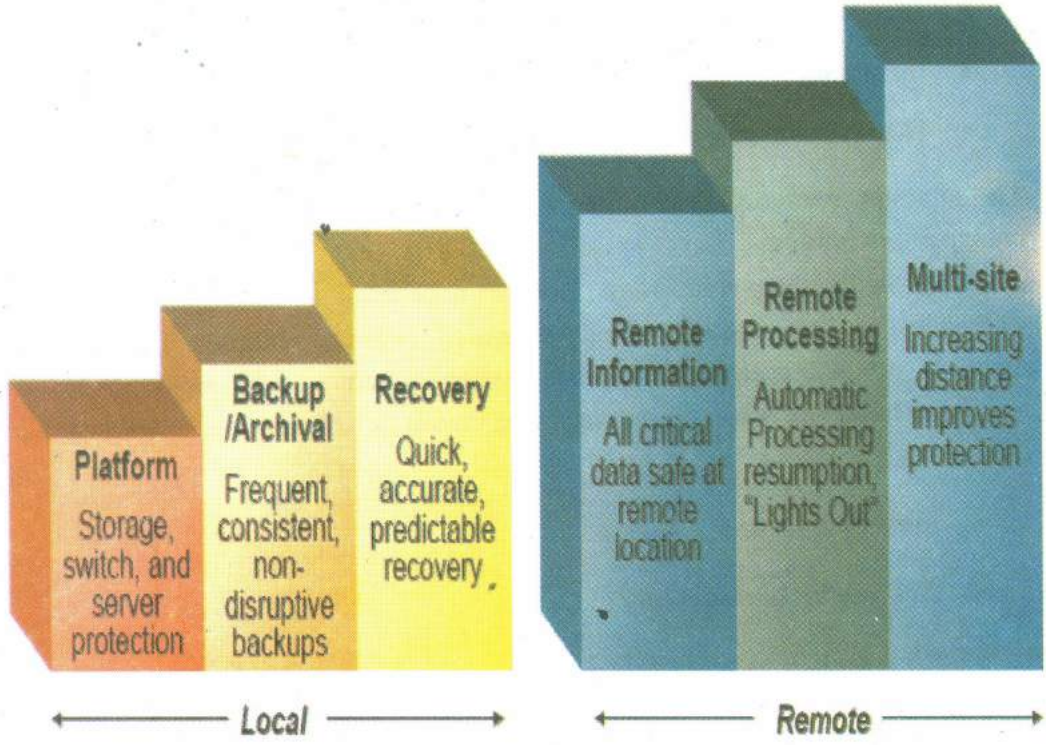

Fig. 2: Application and data restore

1.3 DISASTER RECOVERY PLANNING

Disaster recovery planning describes IT recovery. Some companies use different terms to include the recovery of IT systems, data, information management systems and processes, and other related systems. Depending on the business functions being performed and their dependence on IT, some portion of the critical business processes can be recovered without IT or information. In other cases, IT systems and information are needed to support the recovery of some critical business processes. Each organization must determine the maximum downtime of IT systems that can occur before it becomes an issue that could risk the entire organization, whether it be hours, days, weeks, or more. IT systems include:

- IT data center.
- Applications and data needed by the organization.
- Servers and other hardware.
- Communications such as phone, radio, etc.
- Network, including external (third party) connections.
- IT infrastructure (e.g., logon services and software distribution).
- Remote access services.

- Process control systems (e.g., SCADA/DCS).
- Information management systems
- Document management systems (electric and manual).

The disaster recovery document should describe the IT and information management systems recovery strategies. The DRP should cover detailed recovery instructions that may include references to procedures, vendor references, system diagrams, and other related recovery materials. The detailed recovery procedures must be updated when system and business processes change. Below are some continuity issue that may be recovered as part of the DRP.

- Survive a disaster
- Achieve high availability
- Prevent data corruption
- Non disruptively upgrade software and/or hardware
- Do parallel processing
- Move and migrate data
- Restart the enterprise
- Protect remote data sites
- Shorten backup and restore times
- Contain costs

1.3.1 Risks and Threats

Technological advancement like Local Area Networks, Wide Area Networks and wireless network, made data widely available to users. With small mismanagement, the same data will be accessible to unwanted users hence can create immediate problems to the Business Continuity. The Tender Document, which one has planned to submit next day with little efforts, can ruin the business targets of the year. Making the desired data at desired time is most important part of Business Operations. Securing Network traffic, files and stopping External intrusion are the part of BCM. Cold sites, Warm site and hot sites are the major modalities apply on data broader availability for Business continuity in case of any disaster.

Explosion of Data

In fact, data is easier to create than to Manage, secure and administrate. Just of small network of users, carry several formats and types of data traveling

spontaneously. Application's data (Entered by an application on any Database like Oracle, SQL DB), Documented Data (Quotations, Proposals, Inquiries, Contacts) Emails (PST files) and various independent applications are depending source of any IT Operation. All Businesses depending on any sort of Computers in Operation are equally important to the business. Managing these data is a thorough activity, and making this data available in case of any disaster is serious responsibility. While applying BCM on IT segments, following are the risks, to be addressed comprehensively.

- Send mail Buffer Overflow
- Global file sharing (NetBIOS, Macintosh web sharing, UNIX NFS)
- Use of weak password or no password on user id
- Viruses and worms
- Human error
- Employee sabotage
- Hackers
- Power outages and infrastructure issues
- Natural disasters
- Terrorist and other attacks
- Hardware and software failure

1.3.2 Determining Risk Factors

Business resilience has become a top priority for both executives and stakeholders, and with good reason. An increasingly interconnected marketplace means that any enterprise, at some point, is likely to be vulnerable to risks beyond its control. Any number of these risks factors—whether down the supply chain or in another corner of the world—could endanger business and its reputation.

To meet the uncompromising expectations of the clients, the infrastructure, data and people that comprise business must be reliable, agile, resilient and secure. As the number and types of risks continue to grow, a robust business resiliency strategy is essential to determine the risk for the company's future success and strategy to address the complex business challenge and develop a DRP plan that flexibly meets organization's changing needs. DRP must be interdisciplinary, enterprise-wide business resilience strategy that proactively anticipates and effectively responds to the risks.

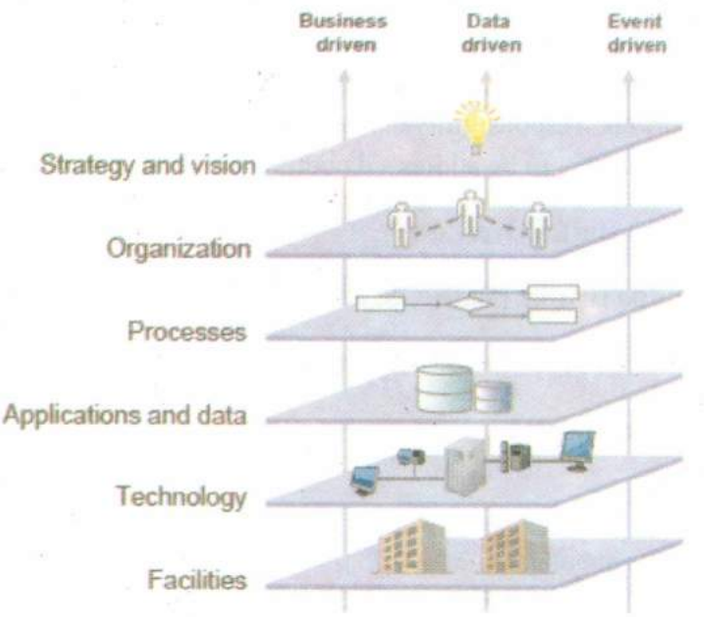

Fig. 3: Business resilience

Business-driven risks: It is affecting business continuity and strategic business operations, business-driven risks—including application outages or overload from marketing demand-generation campaigns—may create enterprise-wide ramifications that result in breaches in compliance, governance, availability, security and performance. They may also invite unwanted intrusions into critical business services. Left unaddressed without a business continuity plan, they cause intense concern for executive board members and other stakeholders. A robust resiliency solution can help to protect organization from this type of risk. It goes beyond simply restoring IT infrastructure, to also helping keep business continuously operating and easing management of compliance with industry and government regulations—so virtually anytime, anywhere accessibility to approved users can be provided.

Data-driven risks: Overlapping with business-driven risks, data-driven risks apply to all data and are caused by a wide range of factors, including disk failure, corruption, viruses or even extreme data growth. Such factors negatively impact continuity as well as the infrastructure, processes, people and systems that keep organization's data and information accessible for business operations, compliance audits and legal requests. To protect against data-driven risks, solution is needed that delivers efficient backup and quick retrieval of critical data and information. There is a need to index, search and retrieve archived information, whenever and wherever it is needed. It must be ensured that data is managed continuously and is safe from viruses, theft and other types of loss.

Event-driven risks: Disrupting an organization's workforce, processes, applications or infrastructure, event-driven risks are caused by power outages, natural disasters, pandemics, fires, thefts and other IT disruptions, including those created by mergers and acquisitions. To mitigate these risks, organization must be able to distribute operations beyond the area of immediate impact as well as implement an effective disaster recovery and crisis management plan. This strategy can keep critical resources, networks, IT services and facilities safe and available to meet the recovery objectives of business.

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 understand with DR

.....

.....

.....

.....

2) What is Business Continuity Planning?

.....

.....

.....

.....

3) What is a business interruption?

.....

.....

.....

.....

4) What is the business continuity management process?

.....

.....

.....

.....

1.4 BCM STRATEGIES

The business unit will be able to choose the appropriate continuity strategies to enable it to meet its recovery objectives. The following items must be included as part of the strategy:

- Staff
- Premises (alternative working arrangements)
- Technology
- Information
- Suppliers
- Stakeholders

1.4.1 Determining Outputs and Deliverables Services and Products

As illustrated in the following diagram, where a decision has been made to include Product A in the scope of the BCM programme and exclude Product B. This means that the activities that support the delivery of Product A (Activity 1, Activity 2, and Activity 3) are In Scope, whilst the activities that do not support the delivery of Product A (Activity 4 and Activity 5) are Out of Scope.

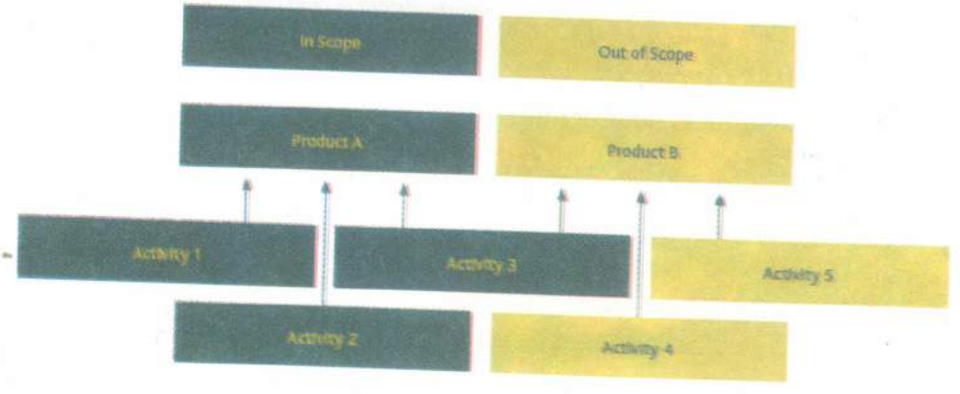

Fig. 4

1.4.2 Call Centre (s)

A convergence of IT, voice recording and intelligent telephony in a call centre may provide significant recovery challenges. Due to the typical staff make-up of this type of facility during a sustained period of outage this can present manpower challenges in the event that staff is unwilling or unable to relocate. Some service companies can provide call answering with varying abilities to handle call volumes at varying level of product competence.

1.4.3 Electronic Commerce and Internet / Intranet Strategies

These will have a choice based on how the whole organisation views the importance of these services and the role they play - whether for communication only or for interactive business. The resumption parameters of Electronic Commerce Services need to be determined by a Business Impact Analysis in the same way as other functions. Electronic Commerce Services are often seen as needing rapid resumption because of their visibility and customer expectations. The Internet and Corporate Intranet may also provide an excellent vehicle for communications during an incident.

1.5 DEVELOPING AND IMPLEMENTING A BCM RESPONSE

This phase of the lifecycle is concerned with the development and implementation of appropriate plans and arrangements to ensure continuity of critical and other activities and the management of an incident. An Event/Incident/Crisis (E/I/C) response structure and plan must be documented and in place to enable an effective response and recovery from disruption. Such response plans include Business Continuity Plans, Technology Recovery Plans and Crisis Management Plans

1.5.1 Business Continuity Plan

The core document, carrying all these information and Planning, will be Business Continuity Plan (BCP-Manual). This document brings together the actions to be taken at the time of an incident, who is involved and how they are to be contacted. The plan or plans must reflect the current position of the organization and all it stakeholders. A BCP should be designed to provide recovery of the organization within the recovery time objectives established during the BIA process. In developing of the plan consideration must be given to:

- The use of planning aids, plan development and maintenance tools
- Inclusion of job descriptions for those involved in delivering the plan
- What action plans and checklists should be provided
- What information databases and other supporting documentation are required
- The recovery team description, responsibilities and organization
- Support staff required including recovery and group co-coordinators
- The location and equipping of the Emergency (Crisis) Operations Center

BCP is more a continues process than a generic Plan, so regular research and amendments in the plan is the most appropriate factor to make the plan practically applicable, in case of any disaster. Specialized Consulting is also available for these segments from various companies within the region.

1.5.2 Resource Recovery Solutions and Plans

Common Backup Challenges

- Performance
  - Not meeting backup windows
  - Cannot provide adequate restore service levels
- Availability
  - Limited reliability of tape infrastructure
- Management
  - Constant tuning of environment
  - Incremental, fulls, etc.
- Data retention
  - Reliance on old backup images for long-term retention

Backup, Recovery, and Archive: Three Separate Challenges

- Production Environment Is Growing
- Growth in the production environment is costly
- Requires more staff for performance tuning, allocation, backup, configuration management
  - Backup Requirements Are More Difficult to Meet

Fig. 5

- Too long to restore
- Backups are not completing consistently
- Tape backup infrastructure is costly and complex to manage Backup
  - Archiving Doesn't Meet New Business Needs

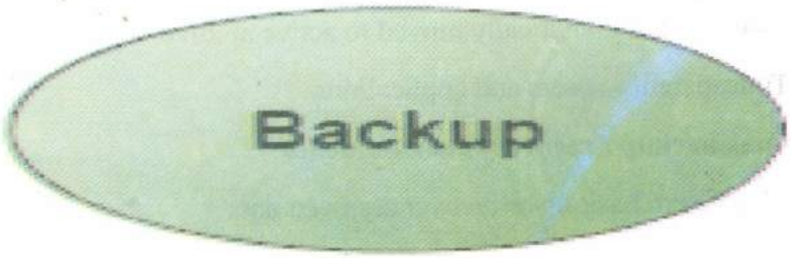

Fig. 6

- Archived data is difficult to access
- Using backup as the archive source causes duplicate data
- Difficult to meet compliance and business practice standards

Fig. 7

Backup, Recovery and Archive

Backup, Recovery, and Archive backup, recovery, and archive improves service levels by speeding backup, recovery, and retrieval of information. Moving unchanging data into an active archive frees up space in the production systems which lead to a 1+1=3 value proposition. You receive the benefits of improved performance and efficiency in production environments, speed backup and recovery processes with backup-to disk, and improve online access to critical information via active archiving

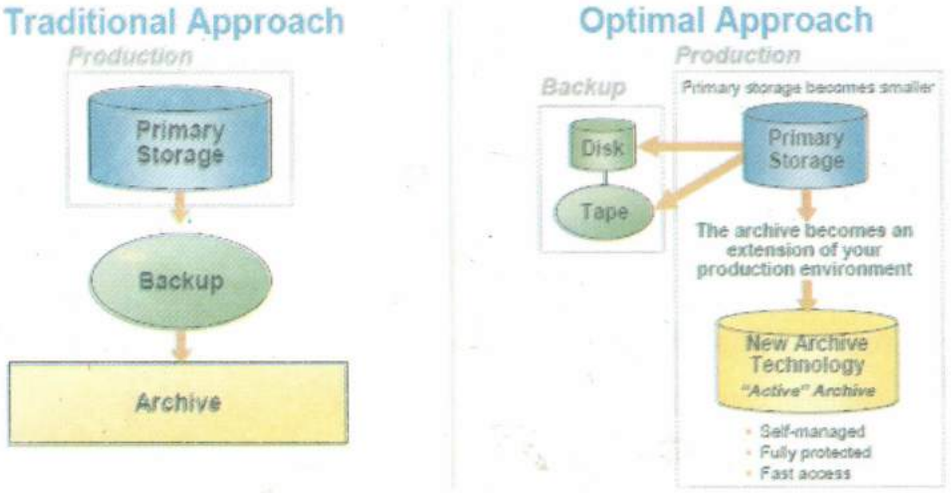

Fig. 8

- **Improved production environments**
  - Static data automatically moved to active archive
  - Transparent to users and applications
- **Shrinks backup / recovery environments**
  - No need to back up or recover archived data
  - Leverage performance and reliability of backup-to-disk
- **Improves access to archived data**
  - Online access supports new requirements

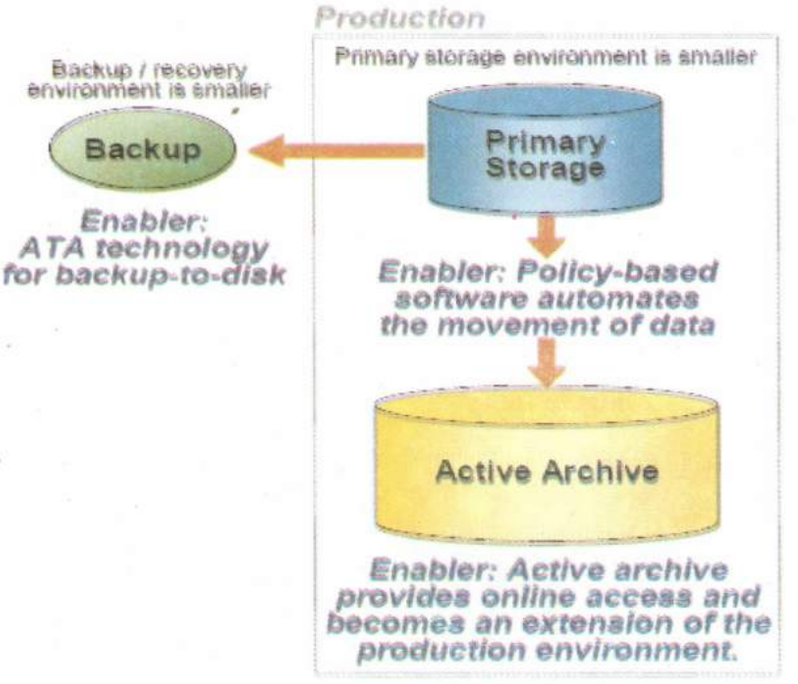

Fig. 9

Backup-to-Disk for Fast Recovery

- Fast restore of critical applications
- Full backup and incremental run at disk speed
- More reliable media
- Speed and reliability benefit of disk based backup
- Operated by traditional tape commands
- No need to change backup management software
- Seamless implementation
- Complements current tape backup
- Non-critical applications continue to use existing tape

- Critical applications leverage disk and can be transferred to tape for offsite storage

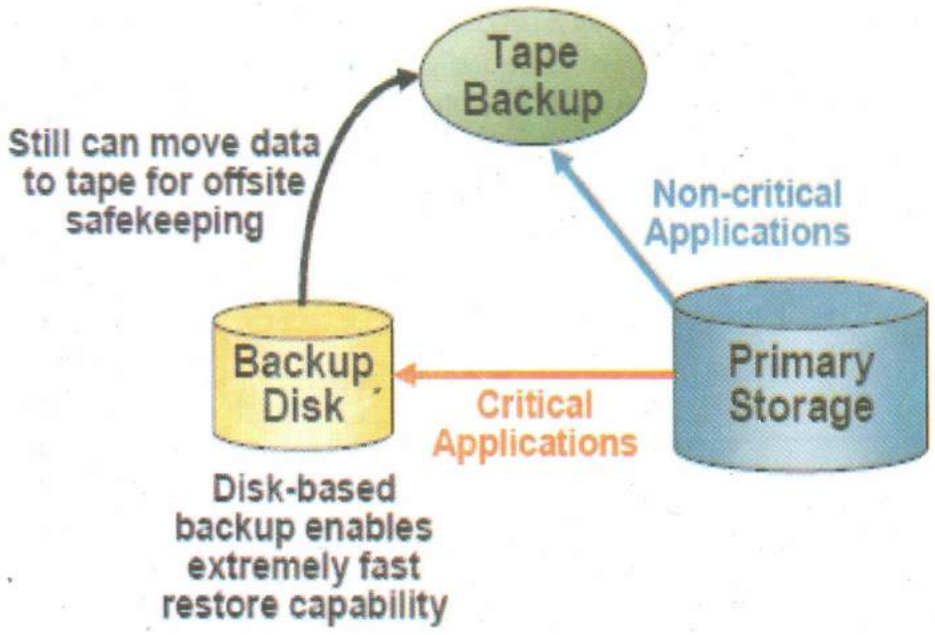

Fig. 10

New Architecture for Backup/Recovery and Archive

- **Archive** valuable information to tiered storage
  - Increases performance and TCO
- **Backup-to-disk** for active production information
  - Much less content, better chance of full backups
  - Backup-to-disk performance, reliability benefits
- **Retrieve** from archive or **recover** from backup
  - Archive information is now available for new business uses
  - Recoveries faster, more simplified

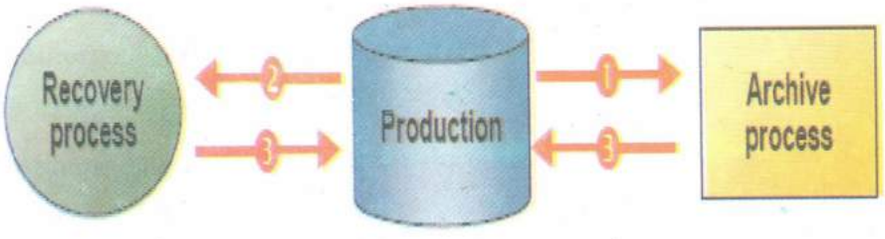

Fig. 11

1.5.3 BCM Awareness and Training

The BCM Policy provides the framework for supporting the requirement for cultural change. Within the BCM culture and awareness activity, the design and delivery of education, training and awareness must be derived from a justifiable Training Gap Analysis. The responsibilities of individuals within the BCM programme need to be assigned before the programme is designed. The purpose of this activity is to define the BCM messages to be assimilated by staff, and select the most effective means to deliver those messages. The techniques which might be used include:

- Training – specific BCM related skills
- Education – specific knowledge for BCM issues
- Awareness – general BCM knowledge

1.6 MONITORING DRP

As originally conceived, the Internet was a technological revolution in information gathering and dissemination. High-speed data links and packet switching allowed mail and file transfers between a small group of government and university computer systems. Today, the Internet is a global network connecting tens of thousands of computers and more than 30 million users throughout the world. Any Disaster Recovery Practitioner ("DRP") with access to a PC and a modem can now roam the Internet and gain access to literally thousands of sources of essential disaster recovery and risk management information. With the World Wide Web ("WWW") at their fingertips, DRP's can call-up the Home Pages of organizations which provide valuable information ranging from earthquake preparedness to locating disaster relief agencies. DRP's can download vital information from these Home Pages to create and/or enhance their own contingency planning efforts. Using an Internet Browser, a DRP can access on-line Search Engines to drill-down to topics as specific as hot sites or sources of disaster recovery education. The Internet is truly an indispensable tool for any DRP.

The Internet contains nearly 12,000 sites which hold information on emergency management, risk management, disaster recovery, and security. DRP's can have access to the same information that the major disaster recovery consulting firms do if they invest their time in a little "Data Mining."

DRP's should maintain their own favorite places on the WWW and organize them in the following categories:

- Plan Development Sites, e.g. Disaster Recovery Journal, Insurance Industry Association etc.

- Risk Management Sites, e.g., Hazard Reduction and Recovery Center, etc.
- Disaster Response Sites, e.g., American Red Cross, FEMA, etc.
- Security Management Sites, e.g., CERT, Mega Mall - Safety and Security Document the addresses of all the WWW sites along with all the other emergency contact information.

1.6.1 Backing Up/Restoring Critical Data

Backing up PC and network data is certainly nothing new. However, using the Internet as an enabler to backup and restore critical data is relatively new. A number of companies have already emerged offering services for backing up and restoring data over the Internet. Subscribers to these services would download the backup/restore program from a service providers WWW site, and then register on-line. Once registered, users would specify a daily backup schedule, after which the service would begin performing the on-line backups automatically. The backup can also occur over a private dial-up network if access to the Internet is not available. Multiple passwords as well as DES encryption to ensure data security are an integral part of these services. The client's data is stored at case-hardened mirrored operations centers, each with multiple levels of data redundancy. In the event of a disaster, users could retrieve their backed up data over the Internet and restore it at a hot site or other recovery location. Costs for these types of services are usually based on the quantity of compressed bytes of data backed up and type of archival media (CD-ROM, DAT etc.).

Commercial Internet Recovery Services Emerge

Recognizing both a financial opportunity and market need for a recovery solution designed around the Internet, hot site providers are now rolling-out Internet recovery services. IBM was one of the first to announce an Internet recovery service through their partnership with Icon CMT Corp., one of the largest Internet Service Providers in the United States. IBM's service is designed to recover WWW applications in the event of a disaster. Through their offering, IBM can reestablish the connection to the client's critical Internet-based applications, allowing the client's user community to continue to access the applications following a disruption. IBM provides the network equipment that enables the client to connect their systems to the IBM network.

1.6.2 Internet Security Concerns Abound

One of the most publicized aspects of the Internet has been the universal concern over the lack of security. There are two primary security concerns associated with the Internet. The first involves concerns over the threat of hackers accessing the company's system through the Internet connection. The second involves the sanctity of the data once it is sent across the Internet and

who can actually view and/or intercept it. These concerns are certainly not unfounded as stories of hackers breaching Internet security continually hit the front pages.

One of the more famous incidents was Kevin Mitnick's hack into the Internet Service Provider Netcom Communications Corp. in San Jose, CA where he stole over 2,000 credit card numbers. The most effective way to protect the company from outside intruders is to implement a fire wall at the company site. Fire walls range in sophistication from simple protocol filters which restrict data traffic to and from the Internet, to advanced fire walls which control the types of packets that can actually move in and out of the system. If the concern leans more toward the security of the data being transmitted, data can be encrypted at multiple levels. Security measures include securing traffic between network nodes using Internet Protocol ("IP") level encryption software or encrypting data at the session level by securing the Sockets to ensure that text and graphics can be encrypted prior to being sent to a browser.

As the company's DRP, it must work closely with the security administrator to assess the vulnerability of the company's network and then implement a risk reduction strategy and program to identify and then mitigate breaches in security. Remember, in a networked world, the most likely risks have to combat will be breaches in security, not natural disasters.

Viruses on the Internet

Computer viruses are becoming a growing concern on the Internet. Gone are the days when virus writers were simply amused by developing infectious programs which would spread inside computer programs or the boot sector of a floppy disk. Today, there are new, insidious forms of viruses which attach themselves to programs or files downloaded using FTP's that are invading clients and web sites alike. Internet virus software is designed to run as a dedicated scanning station which is positioned behind the fire wall. This new generation of virus software checks FTP (File Transfer Protocol) downloads and SMTP (Simple Mail Transfer Protocol) e-mail. The emergence of these new anti-virus packages is a direct assault on the unconstrained macro viruses which are wreaking havoc on networks throughout the world. Some cases are as under -

Case 1: Could The Internet Service Provider Disappear? Imagine receiving a phone call one Saturday morning and being awakened with the news that the company's Internet access no longer existed. That's exactly what happened recently in Salt Lake City, UT as the sudden demise of InteleNET, a local Internet Service Provider ("ISP"), left 1,200 companies without the ability to read their e-mails or their customers the ability to access their web site's Home Pages.

Case 2: In Atlanta, GA when Random Access, another local ISP was robbed at gun point while stunned employees watched as the thieves pillaged every web server in search of their memory chips. Random Access estimated the loss at nearly $1 million. In this case over 500 companies lost Internet access for nearly a week. Although few companies have placed their strategic applications on the Internet, many do nonetheless rely on the Internet.

If the company is among those that do, you need to have a recovery strategy in place in the event that the company's ISP disappears. First begin by checking the financial background of the ISP the company currently uses and make it a biannual procedure if the ISP is a startup. Next, have the ISP provide you with a copy of their disaster recovery plan to verify if they could (at the very least) survive the most likely outage scenarios. Focus in on how the Home Page and account information is backed up. Request that you also receive backups of any critical web site data. It would also be prudent to have a relationship with a secondary ISP that you could quickly switch to in the event the primary ISP experiences a disaster. Ensure Home Page compatibility and have a procedure in place to notify the clients through an e-mail broadcast or other form of communication of the new number and address at which they can contact you.

Check Your Progress 2

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

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

1) What is Business Impact Analysis?

.....

.....

.....

.....

2) How do you undertake a risk assessment?

.....

.....

.....

.....

3) What sort of risks should be considered?

.....

.....

.....

.....

4) How often BCM plan should be exercise / test?

.....

.....

.....

.....

1.6.3 Maintaining and Administering BCM Plans

This phase ensures that the BCM arrangements are validated, that documentation is a reflection of the current business environment and that the plans are up to date. Key activities are:

- Testing and exercising Business Continuity Plans including Call Trees and Crisis Management Plans
- Maintenance of Business Continuity Plans (and all BCM documentation match current business requirements)
- Review of, and adherence to BCM Policies and Standards

Firewall architectures – a look at some critical system platform issues

Imagine a LAN as a building with its size in proportion to the computer network size and capacity. The building has its offices – workstations, store rooms and archive rooms - servers, corridors that connect various building segments – routers. When implementing a defensive system for building security, the designer must plan the positioning of firewalls in advance so that they will be able to block a fire and protect as much of the building structure as possible. It's obvious, that all walls of the building might be made of a firewall technology, but the costs involved would become magnified out of all proportion. Therefore, when considering firewall deployment, the designer must well address the following question: "From where would a threat to the system most likely originate and for what reasons?" Once the places of potential origin of the fire have been determined, the designer can attempt to make a layout of firewalls. The designer of a building is allowed to be free from the fear that a disgruntled employee might set off a fire in the office using the furniture, whilst on the other hand the firewall designer will have to take into consideration such events.

Many users inside the protection of a firewall believe that their systems are safe, since the firewall sits between the LAN and the public network. This is risky thinking; because firewalls are perimeter security only (even those being equipped with "true" firewall features) and once bypassed provide little or no security. The security policy must determine how basic communication will take place at the firewall, where the firewall must sit and how to configure it.

The security policy should also define if more than one firewall is required (or maybe, that a firewall would be of no use) and what should the connectivity scheme be. Once installed, a firewall system is an ongoing process that requires constant vigilance, maintenance, log reviewing and response to events. The inability to keep these requirements satisfied, and sometimes made worse by an inadequate or poor administration that would weaken any protection provided by even the best firewall, would result in it becoming nothing but a murmuring and flashing electronic box, yet adding the danger of providing the illusion of security that can further erode the private network itself.

Risks

A firewall is primarily used to protect the boundary of an organization's internal network whilst it is connected to other networks (e.g. to the Internet). A typical misconception is, as I already mentioned, to use perimeter routers for performing this role. At the very least, perimeter routers can be employed in two ways: either without packet filtering rules involved or by using an IP filtering router solution (most likely together with a dynamic NAT) selectively passing or blocking data packets based on port information or addresses acceptable by the security policy. A firewall must always be situated next to the router. Some practical solutions to this are illustrated in Figures below.

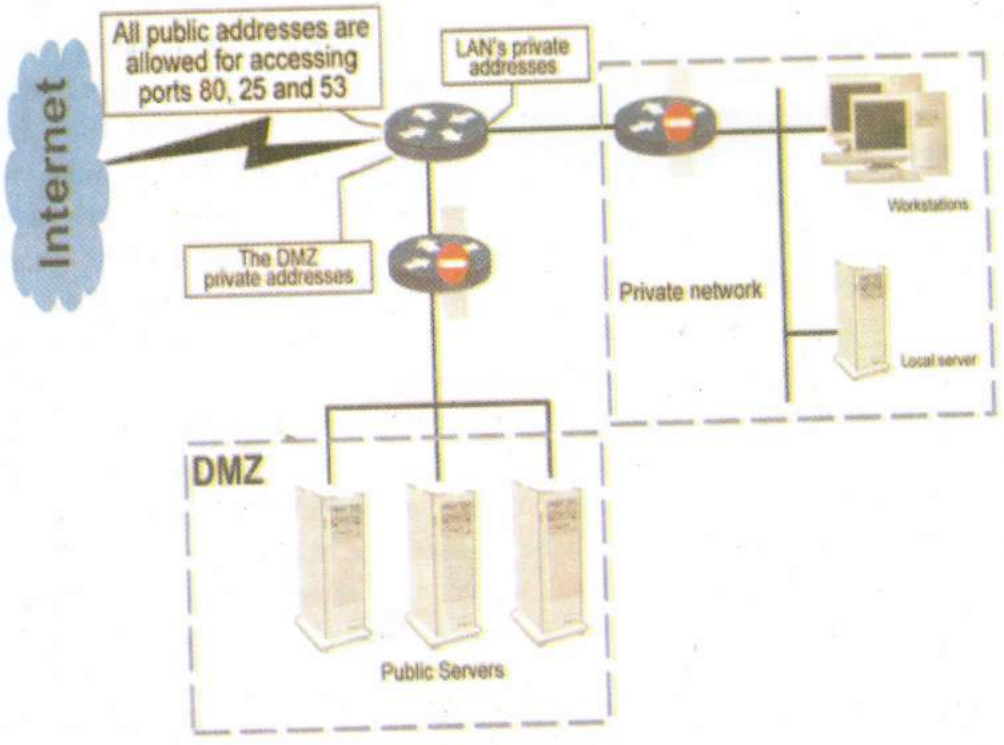

Fig. 12

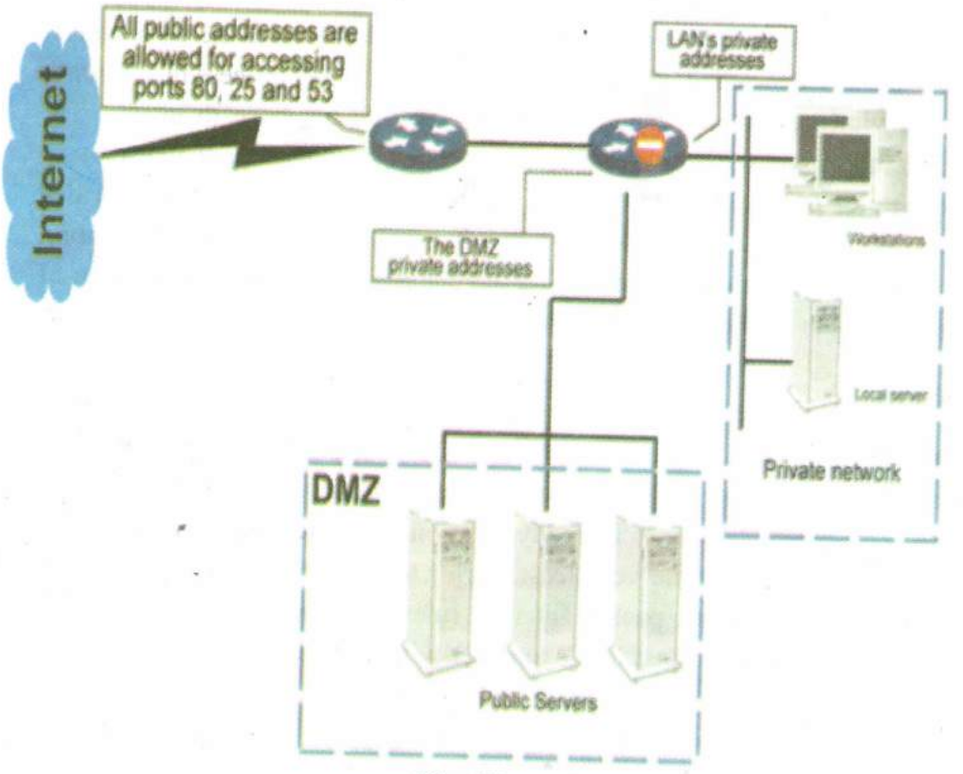

Fig. 13

In these examples, a perimeter router controls traffic at the IP level. This device should be considered the first (but not only) line of defense protecting a private network. In implementing the packet filtering services should be placed inside private networks (that separate two networks) primarily to block unwanted packets accessing other LANs. The criteria used in filtering rules for determining the disposition of packets (accept or reject) should be consistent with the specific security policy, not established at the discretion of the system administrator. In each of the figures there is an isolated area called DMZ that stands for DeMilitarized Zone. A DMZ in the IT sense is an interface that enables the network designer to setup different rules of access for both networks separated by a DMZ for better security. Secondly, the implication of â DMZ is clear; an acceptable tradeoff involved here, is that it would be preferable to have a machine that is a more "attractive" target hacked into, for example, the Web server, that may be re-assembled in a few minutes, than it is to have the workstations or local servers that often contain a company's strategic information hacked into. There is a catch however, that with such a solution, because it presents an essential flaw, namely that of a lack of separation between servers and workstations across a private network, insider attacks are more likely to occur or, an intruder may use an internal workstation as a jumping off point for an attack, for example, by email. To avoid this, internal servers should be isolated by extra internal zones protected by a firewall (or more firewalls if so required).

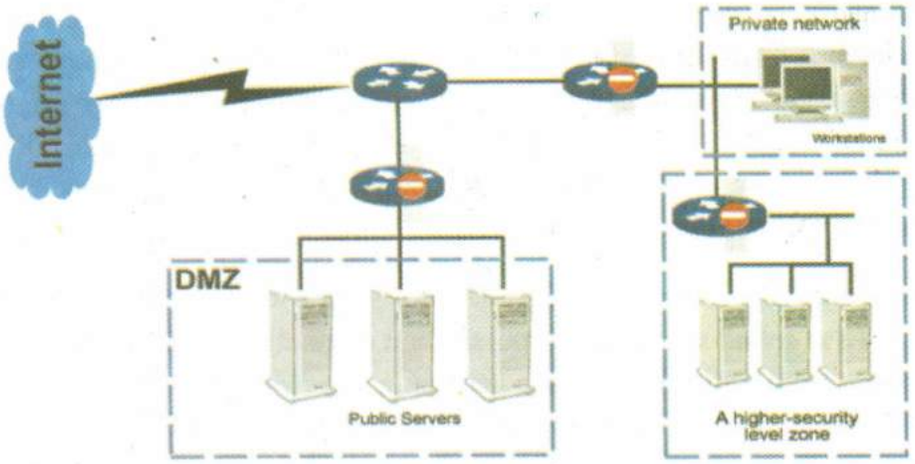

Fig. 14

Such solutions however, are seldom used due to a poor cost-to-benefit ratio. For the servers in private networks to operate effectively, they must be appropriately protected, whilst a consistent security policy should make it impossible to get into protected areas by unauthorized users. In addition, any attempts to break into a private network could be simply detected and restrained using administrative and legal measures. The approach described above seems to be a reasonable means of providing segregation and protective isolation between various internal departments of a large organization, for example to "isolate" a research center in order to protect the research results from being captured by competitors or in large private networks such as academic and corporate networks. Here, the approach is based on physical separation of network boundaries. Figure below illustrates an example of this type of network.

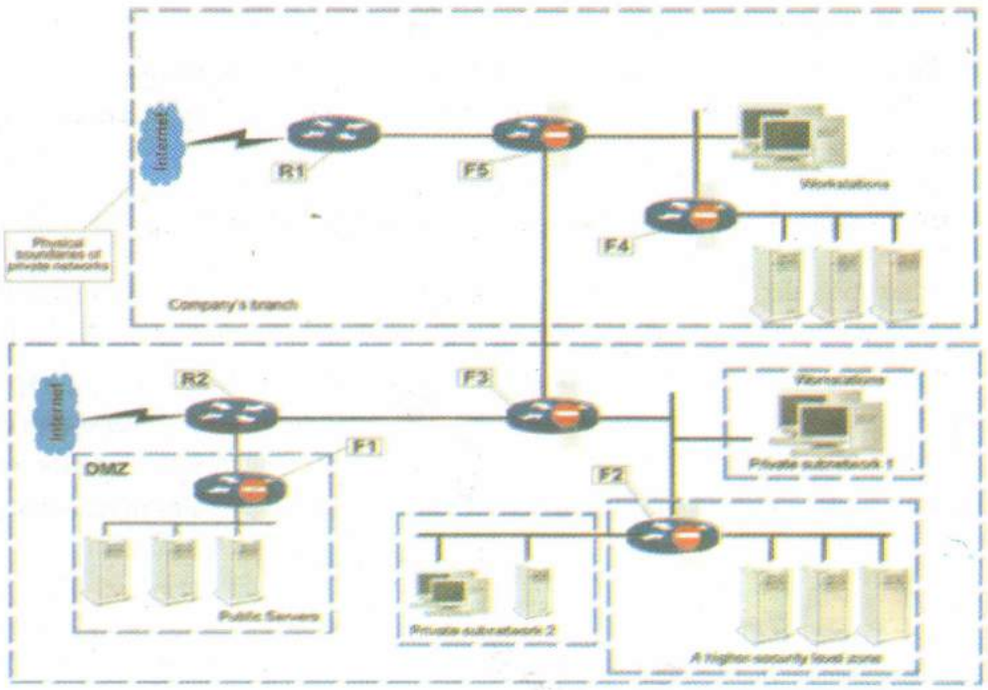

Fig. 15

The R1 and R2 are perimeter routers of a private network. The objective should be to distribute tasks between different devices (following the philosophy: "less components, less prone to damage"), let's say, the initial packet filter can (or even should) be made only on the perimeter router, regardless of whether other protective provisions have already been implemented. Also, a dynamic NAT may be deemed necessary to sit on this device (although not always feasible).

F1 – a firewall, that establishes the DMZ access rules where public servers sit. F3 and F4 are provided for dual purposes. First of all, they define a set of rules that control traffic between a private network and a public network moving in either direction. These firewalls provide VPN support for interdepartmental connections. Physically it may be a pair of copper wires, leased from an ISP, a wireless connection or any other means. Also, physical boundaries between private networks are defined by these firewalls. F2 and F5 firewalls perform similar functions within the local networks that they have been installed – they establish rules of internal server access to be followed by private subnets. Additionally, the F2 is to eliminate unuseful traffic between the subnets 1 and 2. They are merely some criteria for weighing the choice of firewall application. The reality is that this is a security policy decision first, and a firewall implementation (if at all) issue second. The solution still does not define what types of firewalls are to be installed across a network. Selection of firewall type and locations should also be consistent with a comprehensive security policy. Finally, the benefit of any firewall depends upon a critical issue that is common for all applications, and which may compromise the reliability of the network as a whole. Typically these solutions are enough but not always perfect: if a public network or a specially protected subnet ceases to be reachable even for a little while, the firewall application fails. In order to avoid this, redundant systems are used by configuring these systems so that, either all of them control both the incoming and outgoing traffic simultaneously or so that they resume operation after receiving a message signaling a failure of the primary system.

Unconventional solutions – how to setup a simple firewall trap

Another specialized application of firewalls exists, that is often presented in the media but with little practical guidelines given on this issue. Many approaches are possible, therefore the drawing below is a merely a preliminary outline of an idea of such a system. It involves constructing a firewalled trap-network. The theory is that a firewall, to be efficient, must very carefully monitor any incoming and outgoing traffic and reconfigure access policy rules in real-time.

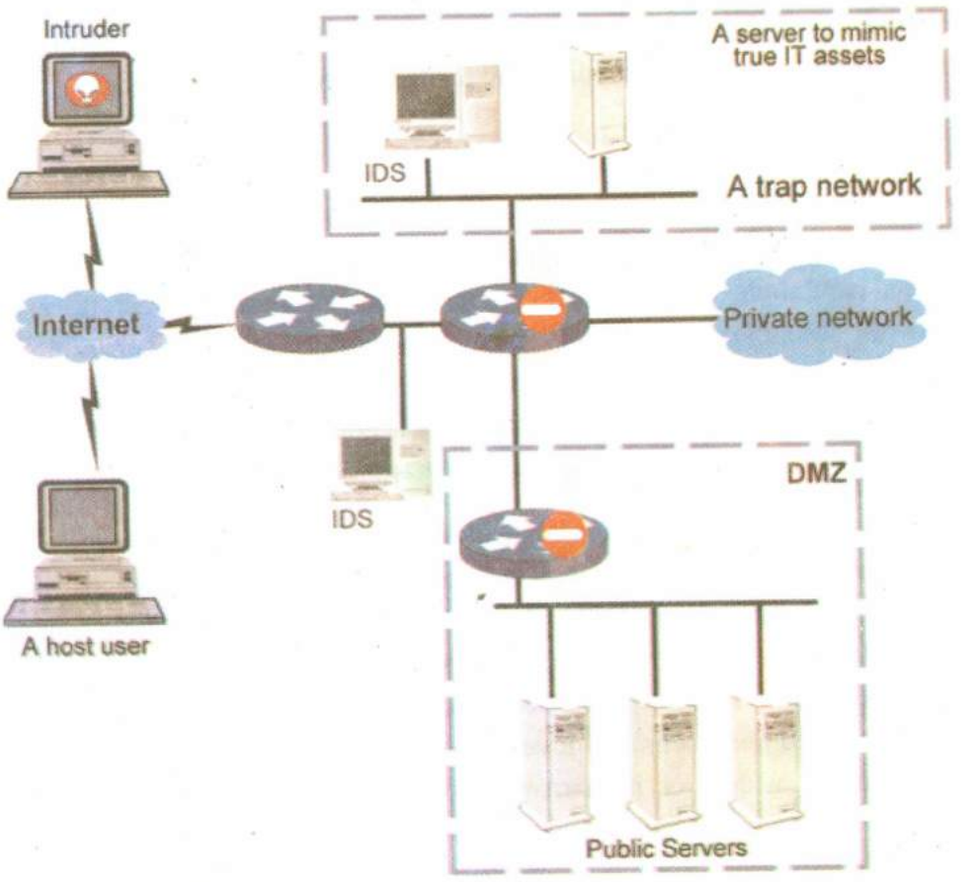

Fig. 16

Suppose a user attempts to get into the company's Web site. Because no malicious intentions are detected, a connection is established. If an intruder were to attempt to access a similar connection, he might begin with scanning the address space of the company. A firewall that is in place detects the hacker's attempt and redirects attacking packets to a trap-network, that may be constructed, for example, by isolating a separate (private) address class on a free firewall interface, so that the dangerous traffic would be transferred onto another network interface. Thus, the intruder enters a server that acts on behalf of the company's Web server. If the intruder neglects to mount a destructive attack for a while, he would probably resume an attack after a certain time, trying to gain access to the "true" server; any hacking action would result in redirecting it to the mimic server, but the consequences (many intruder's footprints) of his attack would be only visible to him and the system administrator. In the figure, there is a device indicated as an IDS (that stands for Intrusion Detection System), which under certain circumstances may operate in a standalone manner and re-configure a firewall with which it operates in conjunction. And what happens if an intruder immediately begins his attack with no scan attempts but directly, by using an exploit technique (most pseudo-hackers use it, in fact)? Of course, such attack would pass through the network gateway, since over here the traffic is not examined at the application layer. With lower-layer based firewalls, only an IDS tool can

provide an effective solution that will be able to automatically re-configure the network gateway, thereby redirecting the traffic to the trap network.

Administering BCM

When the security system identifies an attack, a little common sense and no panic is recommended. An attacker, once scared away, is likely to penetrate the assets next time. If an intruder's actions do not pose a direct threat (e.g. network scanning), do not block them but carefully try to gather information about the attacker and the attack (for further purposes). A more experienced individual may prepare an isolated network segment to setup a trap for forensic analysis and for the undertaking legal steps against the intruder.

The use of central physical repository managed by an enterprise wide document administration strategy for creating, updating, storing, distributing and reporting the status of BCM plans enforces a single authoritative source for every plan and ensures that plans are kept up to date and information that need to be included in multiple plans across multiple offices is more easily updated and distributed and document governance can be enforced. Each plan can then be shared as widely or as narrowly across the enterprise and on different storage devices, according to business need. Administrating BCM plan require the following actions-

- Establish a central repository for all BCM program documents, including BCM plans.
- Version and change management controls should be implemented to ensure that changes are only made to the most current version of the plan. Because plans are usually made up of multiple documents, keeping all the documents synchronized is crucial.
- A tracking method or workflow should be implemented to record which parts of the plan are complete, up-to-date and approved for use, as well as those in the process of being updated and those that need additional work.
- An audit trail, with notices sent to plan owners in some cases, should be kept to record plan document activities, such as plan creation, plan update, plan printing and access to plans that contain confidential organizational information.

The enterprise BCM office is responsible for:

- Administering the central repository
- Facilitating and monitoring the BCM plan update process, that version control is applied and that latest version is distributed.

- Liaising with plan owners to monitor change requirements and the status of changes in progress
- Looking for ways to reduce redundancy
- Enforcing standardization of the BCM plan management strategy and practices

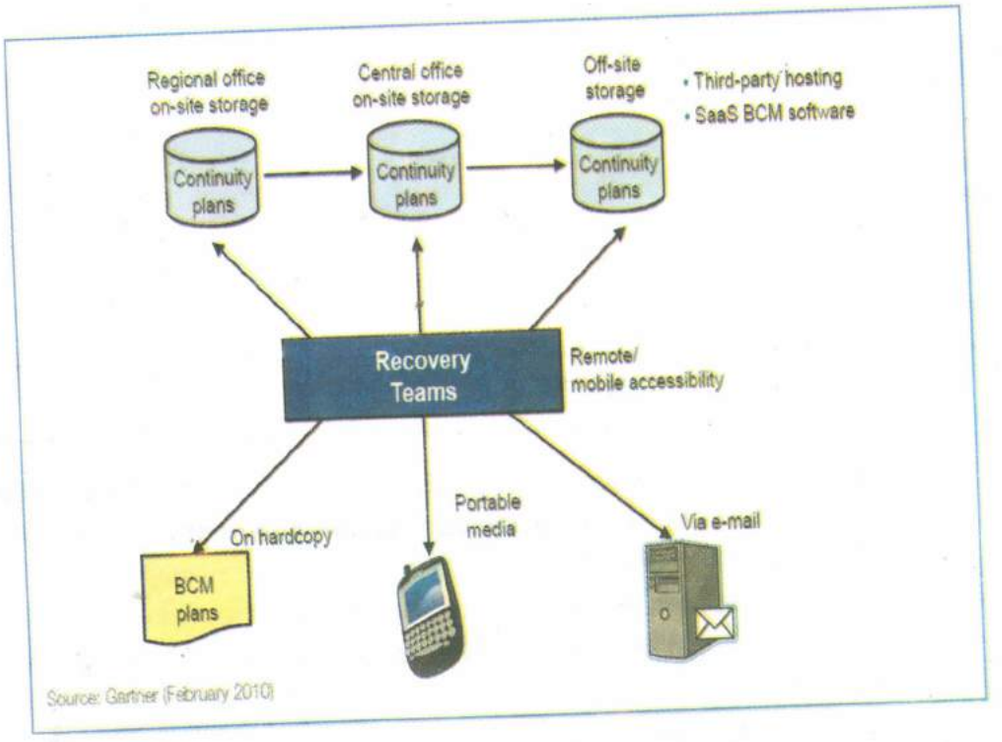

Fig. 17: BCM Plan Storage and Distribution

Check Your Progress 3

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

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

1) What is the scope of a DR test?

.....

.....

.....

.....

2) What is a firewall?

.....

.....

.....

.....

3) What does a firewall do?

.....

.....

.....

.....

4) Is a firewall sufficient to secure my network or do I need anything else?

.....

.....

.....

.....

1.7 LET US SUM UP

BCM is an iterative process, and needs to be actively managed. The initial aim of the stages will be to successfully complete an implementation of the BCM Lifecycle, the long term goal of BCM programme management is to improve the organization's BCM capability, and hence its operational resilience, with successive iterations of the BCM Lifecycle. The early implementations of the BCM Lifecycle will benefit from a project management approach, but as BCM matures within an organization, programme management skills are required to ensure preparedness remains current. A critical success factor is the appointment of competent persons to oversee and manage the BCM programme. The key elements of BCM Programme Management are:

- Assigning responsibilities
- Implementing BCM in the organization
- Project management
- Ongoing business continuity management
- BCM documentation

1.8 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

1) Disaster Recovery or DR is the ability of an organization to provide critical Information Technology (IT) and telecommunications capabilities and services, after it is disrupted by an incident, emergency or disaster. DR recovers the disrupted IT and telecommunications capabilities to ensure

CBFs can continue within a minimum period of time, pre-determined by the organization, to planned levels of operations.

2) Business Continuity Planning is defined by the Business Continuity Institute as 'advance planning and preparation which is necessary to identify the impact of potential losses, to formulate and implement viable continuity strategies, and to develop continuity plans which ensure continuity of organisational services in the event of an incident.'

3) An unwanted incident which threatens clients, personnel, buildings, operational procedures, financial control or the reputation of the Establishment, which requires special measures to be taken to restore things back to normal.

4) The British Standard BS25999 for Business Continuity sets out six elements to the BCM process.

   i. **BCM programme management** - programme management enables the business continuity capability to be both established (if necessary) and maintained in a manner appropriate to the size and complexity of the organisation.

   ii. **Understanding the organisation** - the activities associated with "Understanding the organisation" provide information that enables prioritisation of an organisation's products and services, identification of critical supporting activities and the resources that are required to deliver them.

   iii. **Determining business continuity strategies** - this allows an appropriate response to be chosen for each product or service, such that the organisation can continue to deliver those products and services at the time of disruption.

   iv. **Developing and implementing a BCM response** - this involves developing incident management, business continuity and business recovery plans that detail the steps to be taken during and after an incident to maintain or restore operations.

   v. **BCM exercises, maintaining and reviewing BCM arrangements** - this leads to the organisation being able to demonstrate the extent to which its strategies and plans are complete, current and accurate and to identify opportunities for improvement.

   vi. **Embedding BCM in the organisation's culture** - this enables BCM to become part of the organisation's core values and instils confidence in all stakeholders in the ability of the organisation to cope with disruptions.

Check Your Progress 2

1) Business Impact Analysis is a management tool to assess types of business interruptions, e.g., fire, power outage, etc and the associated consequences over time. E.g., IT failure of several hours may not be critical, but a prolonged IT failure, such as a week, may have significant consequences.

2) Risk assessment is a continuous process that documents the following: identification of hazards, assessment of potential harm; evaluation of existing precautions; review and revision as necessary. The City Council's website contains web pages on risk management. The Health and Safety Executive website can also be accessed for useful risk management publications.

3) The government's UK resilience website lists the following generic risks that should be considered as part of BCP development, in addition to any sector specific risks:

   - large-scale temporary absence of staff;
   - permanent or long-term loss of staff;
   - denial of site or geographical area;
   - flooding;
   - severe weather;
   - loss of mains electricity;
   - disruption to transport;
   - loss of mains water and sewerage;
   - loss of availability of oil and fuel;
   - loss of telephone/ mobile telephone communications.

4) Exercises and testing of BCM plans is an essential part of the process as this will evaluate the viability of the plan, identify areas for improvement and provide training opportunities for staff that may be required to act outside of their normal role as part of BC plan activation. Unworkable plans are as bad as no plans at all. It is usual for "full deployment" tests should be performed, as a minimum, on an annual basis. There are of course other "trigger points", for example, a change in the infrastructure that affects the disaster recovery strategy, i.e. moving from active/contingency recovery model to an active/passive recovery model.

Check Your Progress 3

1) The scope will very much depend on the maturity of the DR strategy and capability, it is important to scope the test to stretch the objectives and success criteria of the previous test, for example, if this is the first test, you

may not want to have the entire user community scheduled to come in and perform lots of testing, you may wish to limit the scope to just IT staff and maybe a couple of "friendly users" to test functionality. Depending on the complexity of the environment it may take several tests to build confidence and perform a "full deployment" test.

2) A firewall protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service. It may be a hardware device or a software program running on a secure host computer. In either case, it must have at least two network interfaces, one for the network it is intended to protect, and one for the network it is exposed to. A firewall sits at the junction point or gateway between the two networks, usually a private network and a public network such as the Internet. The earliest firewalls were simply routers. The term firewall comes from the fact that by segmenting a network into different physical sub networks, they limited the damage that could spread from one subnet to another just like fire doors or firewalls.

3) A firewall examines all traffic routed between the two networks to see if it meets certain criteria. If it does, it is routed between the networks, otherwise it is stopped. A firewall filters both inbound and outbound traffic. It can also manage public access to private networked resources such as host applications. It can be used to log all attempts to enter the private network and trigger alarms when hostile or unauthorized entry is attempted. Firewalls can filter packets based on their source and destination addresses and port numbers. This is known as address filtering. Firewalls can also filter specific types of network traffic. This is also known as protocol filtering because the decision to forward or reject traffic is dependent upon the protocol used, for example HTTP, ftp or telnet. Firewalls can also filter traffic by packet attribute or state.

4) The firewall is an integral part of any security program, but it is not a security program in and of itself. Security involves data integrity (has it been modified?), service or application integrity (is the service available, and is it performing?), data confidentiality (has anyone seen it?) and authentication (are they really who they say they are?). Firewalls only address the issues of data integrity, confidentiality and authentication of data that is behind the firewall. Any data that transits outside the firewall is subject to factors out of the control of the firewall. It is therefore necessary for an organization to have a well planned and strictly implemented security program that includes but is not limited to firewall protection.

1.9 SUGGESTED READINGS

- BS 25777:2008 – Information and Communication Technology Continuity Management www.thebci.org
- Chris Hare, KaranjitSijan, Internet Firewalls and Network Security, New Riders Publishing, Indianapolis 1996.
- http://www.acp-international.com/partners.html
- http://www.continuitycentral.com/contact.htm
- http://www.dri.org
- http://www.globalcontinuity.com/
- http://www.plan-it-control-it.com/
- Micki Krause, Harold F. Tipton, Handbook of Information Security Management, CRC Press LLC, (electronic edition) 1997.
- Strohl Systems (SunGard), Consultant's Corner: Best Practices for Conducting a Functional Exercise

UNIT 2 AUDITING AND EVALUATING BCM PLANS

Structure

2.0 INTRODUCTION

Business Continuity Management (BCM) is the process of identifying the potential impacts to a business and to provide a resilient framework in response. An effective response safeguards the interests of the key stakeholders, reputation, brand and value creating activities. Impacts could be small scale disruptions, such a system outage or large scale disruptions such as the loss of an entire office due to fire or catastrophe. The aim is to minimize the impact and likelihood of disruptions.

BCM

The key elements within BCM are the Business Impact Analysis (BIA), Risk Assessments, Resumption Activities and Tactics. Documentation is required to

support the process, which includes: Business Continuity Management Policy, Business Continuity Plans (BCP) and Incident Management Plans.

Business continuity management (BCM) is moving progressively higher up the agendas of boardroom executives due to growing regulator, insurer and investor interest in risk management and BCM activity. With increasing pressure across all sectors, BCM has become an integral part of any effective corporate governance framework. Boardroom executives and senior management are thus now expected to provide an appropriate level of business continuity preparedness to better protect shareholder, investor and other stakeholder interests. In this unit, we will try to illuminate understanding about the process undertaken by an auditor when reviewing the BCM process. It details the steps the BCM auditor typically undertakes, and provides practical guidance as to the types of documentation and other supporting evidence required during the process. Additionally, the chapter attempts to dispel commonly-held misconceptions about the BCM audit process. Students, executives, senior management and BCM practitioners will all benefit from the practical guidance offered in this chapter, to assist in planning for and surviving a BCM audit.

2.1 OBJECTIVES

After studying this unit, you should be able to:

- define BCM and Key components of the BCM;
- explain BCM audit, types of audits and auditors;
- identify and use elements of existing audit methodologies to perform the audit of a BCM program
- identify components of a complete BCM program
- identify success factors and risks associated with a BCM program
- define the implementation process of a BCM program in order to evaluate the Business Continuity maturity level of an organisation
- develop an Audit program for a BCM program
- list reasons and benefits of BCM audit;
- explain BCM Standards, Guidelines, and Frameworks;
- explain scope of BCM audits;
- explain legal and regulatory requirements;
- explain BCM audit process;
- list key considerations in BCM audit;
- explain BCM audit concerns and focus; and
- distinguish BCM project management vs. process management.

2.2 DEFINITION OF BCM

Business continuity management is the process by which an organization prepares for future incidents that could jeopardize the organization's core mission and its long-term viability. Such incidents include local events like building fires, regional events like earthquakes, or national events like pandemic illnesses.

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

BCM is to safeguard the interests of its key stakeholders, reputation, brand and value creating activities.

2.2.1 Key Components of the BCM

The key components of the BCM are:

- **Management Support:** Management must show support to properly prepare, maintain, and practice a business continuity plan (BCP) by assigning adequate resources, people, and budgeted funds.
- **Risk Assessment and Risk Mitigation:** Potential risks due to threats such as fire, flood, etc., must be identified, and the probability and potential impact to the business must be determined. This must be done at the site and division level to ensure the risks of all credible events are understood and appropriately managed.
- **Business Impact Analysis (BIA):** The BIA is used to identify business processes that are integral to keeping the business unit functioning in a disaster and to determine how soon these integral processes should be recovered following a disaster.
- **Business Recovery and Continuity Strategy:** This strategy addresses the actual steps, people, and resources required to recover a critical business process.
- **Awareness and Training:** Education and awareness of the BCM program and BC plans are critical to the execution of the plan.
- **Exercises:** Employees should participate in regularly scheduled practice drills of the BCM program and BC plans.
- **Maintenance:** The BCM capabilities and documentation must be maintained to ensure that they remain effective and aligned with business priorities.

2.3 BCM AUDIT

The most general definition of an audit is an evaluation of a person, organization, system, process, project, or product. A BCM audit is an independent evaluation of the business continuity management program or its components by internal or external independent parties. The organizations top management should, at intervals that it deems appropriate, review the organizations BCM capability, to ensure its continuing suitability, adequacy and effectiveness. This review should be documented and can take the form of:-

Types of audits:

1. Internal audits
2. External audits
3. Self Assessments

1. Internal audits
2. External audits
3. Self Assessments

2.3.1 Types of Auditors

There are several types of auditors such as internal auditors, external auditors, and compliance auditors.

- Internal auditors are employees of a company that assess and evaluate its systems of internal control. A business continuity plan is considered to be an important component of an internal control system. To maintain independence, they present their reports directly to the board of directors or to executive management.

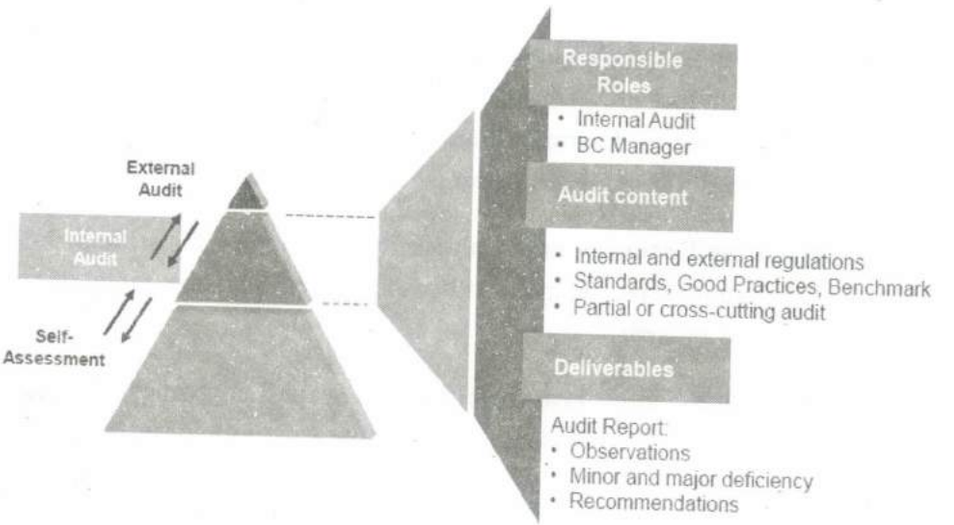

Fig.1 Internal Audit

Types of auditors:

1. Internal
2. External
3. Compliance

- External auditors are independent staff of an auditing firm that assess and evaluate financial statements of their clients or perform other agreed upon evaluations such as IT Audits that may also address the business continuity plans of the organization.

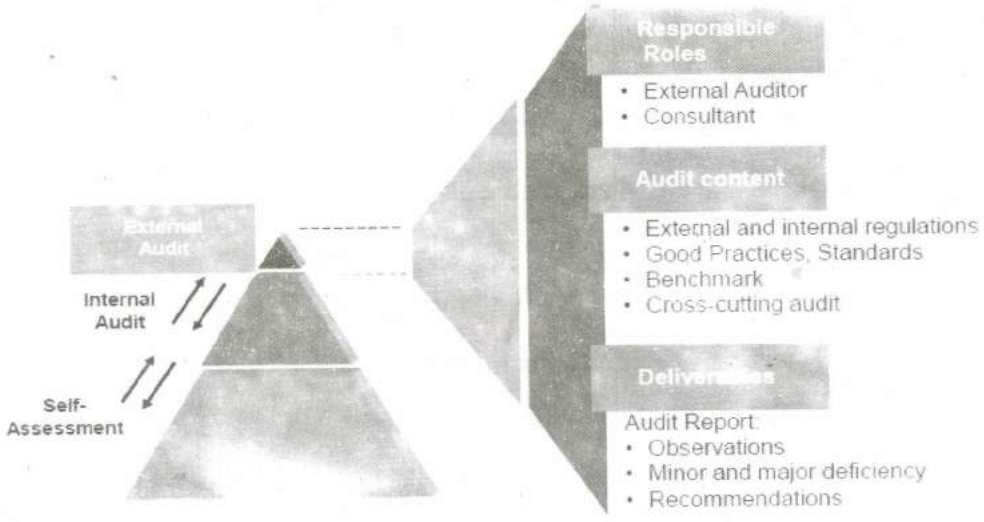

Fig.2 External Audit

- Compliance auditors are examiners normally from a regulatory agency such as FFIEC, FERC, DHS/FEMA, JCAHO/HIPAA, and others depending on the type of industry.

2.3.2 Reasons for the BCM Audit

There are many reasons for BCM audits. The audit may be prompted by the internal audit department, external audit organization such as the CPA firm that performs the financial audit, or a regulatory examiner. Another reason is it may be triggered by the results of an emergency event or by the results of a test exercise. Board and/or executive management may also request an audit of the business continuity management program or components thereof. In some cases a customer may request a BCM audit such as customers of service organizations.

2.3.3 Benefits of a BCM Audit

There are several benefits that can be obtained as a result of a BCM audit. The BCM audit provides an independent evaluation of the BCM program and identification of strengths and weakness of the program. The audit can also reveal high risks and associated mitigation strategies. The results should include recommendations for BCM improvements and identification of "best BCM practices." Few other benefits are:

- Objective evaluation of the BCM Program
- Business continuity office
- Internal and independent
- External and independent
- Alignment with other similar organizations
- Demonstrate compliance and diligence

2.3.4 BCM Standards, Guidelines and Frameworks

The BCM planner may have several questions for the BCM auditor regarding the pending audit such as: what standard will be used for the BCM audit?

There are several BCM standards, guidelines, and frameworks that are used for developing BCM plans including:

- Disaster Recovery Institute International (DRII)
- Business Continuity Institute (BCI)
- COBIT – Control Objectives for Information and Related Technology
- ISO 17799/27000 Series
- National Fire Protection Association 1600 (NFPA 1600)
- BS 25999 (British Standards Institute)
- Various state statutes and regulatory requirements

2.3.5 Scope of BCM Audits

It is advisable for the BCM planner to inquire and understand: What is the scope of the BCM audit? This understanding will help the BCM planner to better prepare the materials needed by the BCM auditor for the audit. The scope could include some or all of the items listed below:

- Business continuity management program and BCM policy
- Enterprise BCM, IT disaster recovery plan, and/or business unit/department BCPs
- Supporting plans (i.e., emergency plan, crisis management plan, pandemic plan, and others)
- Business impact analysis, risk assessment, recovery strategies development, plan design and documentation, training, testing exercises, or all of these phases
- Single points of failure (a single element, component, system, device, or person that is critical to providing a service – availability is the aspect of continuity planning that is concerned with avoiding single points of failure)
- BCM roles and responsibilities
- BCM software (management, access, security)
- Plan availability and updates
- Plan maintenance and evidence of updates
- Plan testing exercises and evidence of testing

2.3.6 Legal and Regulatory Requirements

Both the BCM planner and the BCM auditor should have a solid understanding of the applicable legal standards and regulations and of the organizations making the rules.

- **Health Insurance Portability and Accountability Act (HIPAA)**: Protects medical records and other health information.
- **Department of Homeland Security and Federal Emergency Management Agency (DHS/FEMA)**: Provides guidance for developing Continuity of Operations (COOP) plans as described in Federal Continuity Directive 1 and Federal Continuity Directive 2. These are applicable at all levels of the Federal Executive Branch and are also useful for state, local, territorial, and tribal governments.
- **National Institute of Standards and Technology (NIST)**: Publishes the "Contingency Planning Guide for Information Technology Systems" which provides instructions, recommendations, and considerations for IT contingency planning.
- **Federal Financial Institutions Examinations Council (FFIEC)**: Provides guidance to the financial services industry about the importance of business continuity planning.
- **Federal Energy Regulatory Commission (FERC)**: Regulates the interstate transmission of electricity, natural gas, and oil.
- **Sarbanes Oxley Act of 2002**: Requires management and the external auditor to report on the adequacy of the company's internal control over financial reporting (ICFR). BCM is an important aspect of the internal controls.

Check Your Progress 1

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

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

1) Define BCM and explain briefly its key components.

.....

.....

.....

.....

2) What are different types of auditors in BCM audit?

.....

.....

.....

.....

3) What are the reasons for BCM audit?

.....

.....

.....

.....

4) State the benefits of BCM audit.

.....

.....

.....

.....

5) What are BCM standards, guidelines and frameworks?

.....

.....

.....

.....

6) What are BCM audit and its types?

.....

.....

.....

.....

2.4 BCM AUDIT PROCESS

The BCM audit, like BC planning, implementation and maintenance is concerned with a complex process and requires interaction with a wide range of executive, managerial and operational roles from both a business and technical perspective.

The BCM audit process includes an audit plan, which should include:

- Identification of the type of audit to be carried out e.g. compliance, project management/control, feasibility study, due diligence or investigative.
- Identification of the audit objectives i.e. outcomes and deliverables. The audit objectives may in part be driven and governed or restricted by legal or regulatory requirements. This includes key issues of high priority.
- Identification of the standard audit framework (where appropriate) to be used e.g. NFPA1600. The audit framework may be governed or restricted by legal or regulatory requirements.

Remember BCM audit process includes an audit plan.

- Definition of the audit scope.
- Determine the governance, compliance or other issues to be audited.
- Determine the area/department/site of the organization to be audited.
- Definition of the audit approach and the auditing activities that will be undertaken e.g. questionnaires/face-to-face interview/document review/solution review.
- Activity timetable and due dates.
- Identification of the audit evaluation criteria (standards).
- Determine the requirement for specific subject expertise or third party assistance to conduct the audit.
- Review and information gathering via the BCM audit activities.
- Compile and summarize interview notes, questionnaires and other sources.
- Identify gaps in content and level of information gathered and conduct further or follow up interviews as appropriate.
- Obtain and compare relevant documentation e.g. Business Impact Analysis with interview data and other sources such as walkthrough, physical inspection and sampling.
- Refer to secondary sources e.g. standards, regulations, 'good practice' guidelines to validate preliminary findings.
- Form an opinion that should reflect the interests of the audit sponsor and the 'yardstick' set by external sources e.g. regulatory, legal, industry standard.
- Assign a risk weighting to individual audit item to distinguish between critical, high, medium and low risk findings.
- Define criteria for rating factual findings by using a clearly differentiated categorized predefined rating level.
- Provide a draft audit opinion report for discussion with key stakeholders.
- Provide an agreed audit opinion report incorporating recommendations as well as audit responses where differences of opinion persist.
- Provide an agreed remedial action plan including timescales to implement the agreed recommendations of the audit report. This should also form a key element of the BCM Maintenance Program.

- Provide a monitoring process (in addition to the BCM Maintenance Program) to ensure that the audit action plan to address material deficiencies is implemented within the agreed timescale.

The BCM Assurance process includes:

- Define role accountabilities, responsibilities and authority
- Define Key Performance Indicators (KPIs) objectives, measurement targets and standards.
- Define success factors.
- Incorporate Key Performance Indicators in internal and external contract terms and annual appraisal.
- Evaluate and review performance against Key Performance Indicators, objectives, targets and defined industry standards.

Remember Self-auditing or 'Performance Monitoring' may be carried out more frequently, by the owners of the BC plans themselves.

Methods and Techniques

The methods, tools and techniques to audit an organization's BCM program include:

Audit

Self-auditing or 'Performance Monitoring' may be carried out more frequently, by the owners of the BC plans themselves. The BC Plans are measured against specified performance levels, in topics such as:

- Number of months since last active exercise.
- Number of open-issues still outstanding since last exercise.
- Completeness of the BC plan documentation.
- Number of months since last business impact analysis.
- Number of open-issues still outstanding since last business impact analysis.
- New IT application assessed for inclusion in BC Management Plans.
- New or changed business process assessed for inclusion in BC Management/Plans.
- Adequacy/viability of Recovery Team dynamic data such as team members, contact telephone numbers, notification/supplier list, recovery site workstation allocation.

BCM Assurance

- Creation of a BCM Budget for implementation and maintenance.

- Budgetary control.
- Document analysis and review.
- Self assessment assurance scorecard.
- Interviews.

Outcomes and Deliverables

The outcomes of a BCM audit include:

- An independent BCM audit opinion report that is agreed and 'signed-off' by executive management.
- A remedial action plan(s) that is agreed and 'signed-off' by the executive management.

The outcome of an unfavourable performance rating could be:

- Acceptance of the BC Plans by the Internal Audit department as 'in-adequate'.
- The initiation of a BC review conducted by a third party BC professional to assist the team in improving their position.
- Review of the BCM function.

Review

The policy concerning the frequency of audit should be clearly defined and documented within the organizations 'Audit Policy and Standards'.

2.4.1 Role of BCM Audit Process

The BCM audit process plays a key role in ensuring that an organization has a robust, effective and fit-for-purpose BCM competence and capability. It has five key functions:

1. to independently verify compliance with the organization's BCM policy, strategies, framework and good practice guidelines or standards adopted by the organization.
2. to independently review the organization's BCM solutions.
3. to independently verify and validate the organization's BCP and crisis management procedures.
4. to independently verify and validate that key exercising and maintenance activities are taking place, in line with the relevant programmes, processes and the organization's BCM framework.
5. to highlight key material deficiencies and issues and ensure their resolution.

2.5 KEY CONSIDERATIONS IN BCM AUDIT

The BCM audit, like BCM planning, implementation and maintenance, is concerned with a complex process and requires interaction with a wide range of managerial and operational roles from both a business and technical perspective. The following key considerations should be applied to it:-

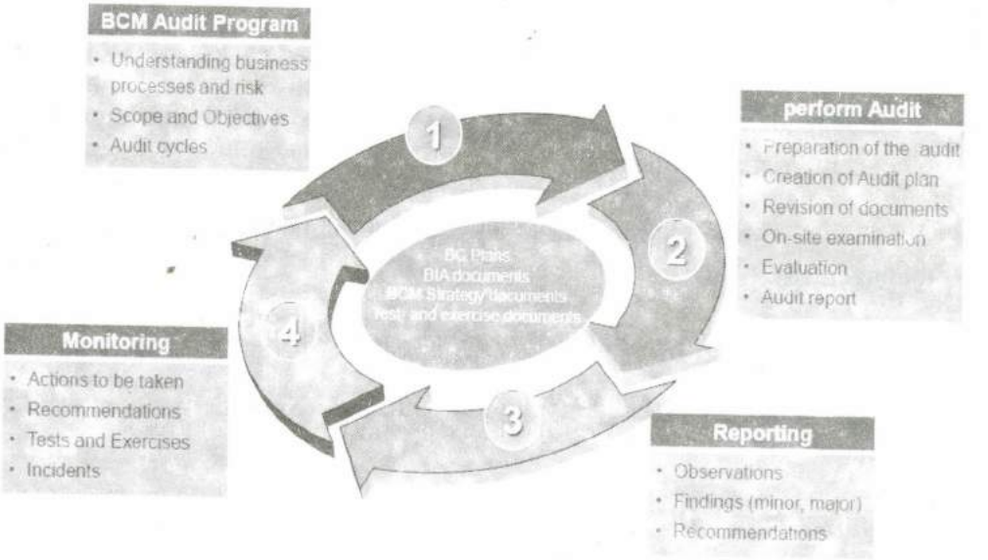

Fig. 3: BCM Audit life-cycle

a. The role and perspective of the auditor and audit function is one of impartial review against defined standards. Whilst the auditor may be fully aware of and may identify the reasons for BCM shortcomings and organizational difficulties, the auditor should clearly identify the BCM competence and capability gaps.

b. An integral part of the audit is to provide remedial recommendations.

c. Each stage of the BCM life-cycle may require a different audit approach. The audit approach is solely dependent upon the maturity of each stage of the BCM life-cycle.

d. A proactive audit process should be seen as an enabling process to achieve a particular management objective.

e. The audit process can be undertaken by an organization's internal audit function, an external auditor, or external professional BCM practitioner. The scope of the audit should be material to the organization, clearly defined, documented and agreed in partnership with the relevant auditee and senior management. Where auditors do not have the requisite professional level of BCM knowledge, expertise and experience, they should employ the assistance of a professional BCM practitioner.

2.5.1 Purpose/ Objectives

The purpose of a BCM audit is to scrutinize an organization's existing BCM competence and capability, verify it against predefined standards and criteria, and deliver an audit report detailing the findings, conclusions and recommendations.

2.5.2 Outcomes

The outcomes from a BCM audit should include verification that:

- issues of operational resilience have been identified and included in the organization's BCM strategies and plans;
- the organization's BCM policy, strategies, framework and plans continue to reflect accurately and be relevant to the organization's priorities and requirements and reflect industry good practice guidelines and standards;
- the organization's BCM competence and its BCM capability are effective and fit-for- purpose and will enable management, command, control and coordination of a BCM incident;
- the organization's BCM solutions are effective, up-to-date and fit-for-purpose;
- the organization's BCM exercising programme is being effectively implemented;
- the organization's BCM maintenance programme is being effectively implemented;
- BCM strategies and BCPs are updated to reflect the lessons learned from the BCM maintenance programme;
- a documented change control process or procedure is in place and operating effectively;
- a clearly defined and documented audit contract and plan (statement of work and scope) is agreed and signed off by the senior management of the auditee;
- an independent audit opinion report is agreed and signed-off by the senior management of the auditee.

2.6 BCM AUDIT CONCERNS AND FOCUS

BCM Auditors may have several concerns related to the BCM as described below:-

- **Risk Assessment**: The BCM auditor may audit the results of the risk assessment as well as the process that was used during the development of the risk assessment to understand if it was comprehensive. The BCM auditor may inquire about the methodology and approach used for the risk assessment. There may be questions related to: analysis of threat and vulnerabilities, physical and environmental security, backup and off-site storage, and single points of failure. In particular, the BCM auditor will be interested in the mitigation strategies that have been implemented.

- **Business Impact Analysis**: The BCM auditor may audit the results of the business impact analysis as well as the process that was used during the development of the business impact analysis to understand if it was comprehensive. The BCM auditor may inquire about the methodology and approach used for the business impact analysis. The audit may review: stakeholder input, recovery point objectives (RPOs), recovery time objectives (RTOs), resource prioritization, potential losses, and interdependencies.

- **BCM Structure and Documentation**: Effective documentation and procedures are extremely important in a business continuity plan. Considerable effort and time are necessary to develop a plan. However, many plans are difficult to use and become outdated quickly. Poorly written procedures can be extremely frustrating. Well-written plans reduce the time required to read and understand the procedures, and therefore result in a better chance of success if the plan has to be used. Well-written plans are also brief, to the point, and meet all project/organizational objectives. A well-organized business continuity plan will directly affect the recovery capabilities of the organization. The contents of the plan should follow a logical sequence and be written in a standard and understandable format. A glossary of technical terms and acronyms can be beneficial in understanding the BCM procedures and documentation. Procedures should be clearly written.

The BCM auditor may audit the BCM structure and documentation. The audit may review activation procedures, communications plan, recovery teams, scenarios, command and control center, alternate facilities, detailed recovery procedures, and other considerations.

The BCM auditor may also ask:

- Where is the electronic copy of the BCM stored?
- Is the electronic copy of the BCM secure?
- Who has access to the BCM and what type of access (read/write/delete)?
- Is there a backup of the BCM and is it stored offsite?

- Are there hard copies of the BCM and are they secure?
- BCM Training: Training is an important aspect in completing the business continuity plan. All employees must know their specific roles in the business continuity plan (BCM) and how to fulfill their responsibilities. Specific training is necessary to maintain, implement, and test the BCM. Training recovery personnel and providing them with multiple skills can weigh significantly on the success of the plan and the time required to execute it. An awareness program should be used to initiate staff training efforts related to business continuity planning and included in employee orientation training and related materials.
- Successful execution of the BCM will largely depend on how well participants accept the importance of the plan, the credibility of the plan, and the degree and quality of the training provided.
- It is essential to provide training for all members of the planning team as well as other key staff. The BCM auditor may examine the training plan, types of training provided, training instructors and participants, content of the training, and training evaluation and results.
- BCM Testing: The plan should be thoroughly tested and evaluated on a regular basis (at least annually). Procedures to test the plan should be documented in a test plan. Testing and exercises provide the assurance that all necessary steps are included in the plan. The BCM auditor may examine the BCM policy statement for the testing responsibilities and requirements. In addition, the auditor may also review the test plan, the participants, and the documentation resulting from the test such as problem logs. Debriefing documentation could also be requested.
- BCM Maintenance: As systems change, the BCM must be updated to reflect those changes. The maintenance procedures should allow for a regular review of the plan by key personnel within the organization. The BCM auditor may examine maintenance logs, maintenance policies and procedures, maintenance roles and responsibilities, frequency of updates, and plan distribution and methods. Some organizations include BCM as part of their change management and control procedures.

2.6.1 Most Common BCM Weaknesses

Some common weaknesses of business continuity plans identified as a result of BCM audits are listed below:

- Often there may be a BCM plan but it may not contain a BCM policy statement.
- Organizations often have multiple types of plans without adequate integration. For example the emergency plan or the crisis management

plan may not be properly coordinated with the BCM. This can result in confusion at the time the plan(s) need to be activated.

- Some organizations have developed comprehensive business continuity plans, but maintenance roles and responsibilities have not been clearly defined. This can result in the BCM quickly becoming outdated.
- There may be a lack of training and knowledge transfer of the BCM. This creates a significant reliance on a few individuals and can result in improper execution of the plan.
- Many organizations perform IT testing exercises but limited testing in other areas. This also can create problems if the plan needs to be activated.
- In some organizations, the IT professions develop the BIA and determine priorities without stakeholder involvement. Although IT professionals often have a good understanding of the business processes, a lack of stakeholder involvement can result in incorrect RPOs and RTOs.
- Many organizations do not include BCM in the change management process. This can result in the system being implemented without a recovery strategy.
- Some organizations have developed good recovery strategies but have not documented the procedures to support their strategies.

2.6.2 Road Map for BCM Audit Success

The following recommendations will help to ensure the success of the BCM planner in connection with an audit:

- Understand the scope of the audit and underlying standards.
- Assure that all BCM documentation is up-to-date.
- Assure that all phases of the BCM development process have been performed and documented.
- Assure that there has been adequate training on the BCM and supporting documentation.
- Assure that the plan has been exercised and debriefing documentation has been completed.
- Work with (not against) the BCM auditor.
- Obtain value from the BCM audit.

2.7 BCM PROJECT MANAGEMENT VS. PROGRAM MANAGEMENT

Often, corporations believe that by implementing a BCM project the entire program and related deliverables will be established and ready for use when a disaster strikes. What gets forgotten is that it takes numerous BCM projects to establish a proper program, each with its own set of objectives and deliverables. Many corporate executives don't understand between BCM projects and a BCM program but there are differences that need to be addressed and known if the BCM program is to be successful.

Below is a short list of differences that will help BCM professionals and corporate executives understood the differences if they're working with a project or helping establish a program.

1. A project is unique, delivers a specific output, or deliverable, and has a specific start and end date and must meet strict criteria such as time, cost, satisfaction, quality, scope and risk; sometimes referred to as the "Triple Constraint" derived from the original three constraints of Time, Cost and Quality. In contrast, a program is ongoing and designed to consistently achieve specific goals for the business.

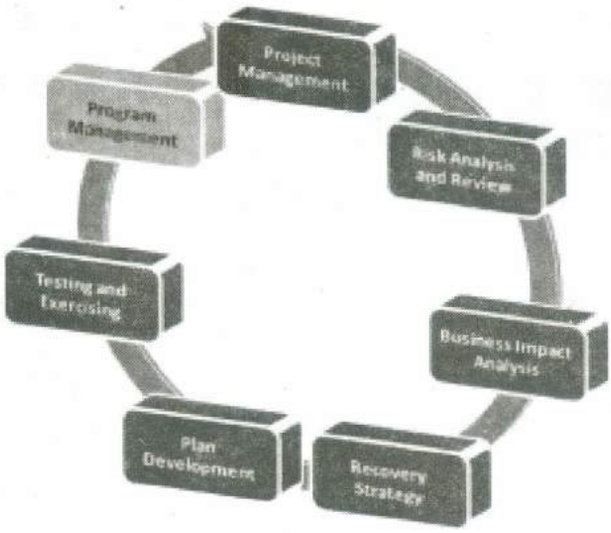

Fig. 4

2. Program management includes management of projects that when combined improve the viability, performance and the day-to-day operations of the organization.

3. Project Managers will manage individual projects with specific goals and objects and a PM may be responsible for more than one project at a time. The Program Manager may be responsible for the coordination of multiple PMs who are responsible for the program and report to a program sponsor, who is usually at the Executive level.

4. Projects may change in size and scope but are still responsible for delivering specific deliverables based on time, cost, quality, risk, satisfaction and scope. Of course, proper project change management procedures would be utilized to ensure that when scope changes, the impacts are identified on the remaining 5 components noted in the previous sentence. Programs change however, when the organization changes or the strategic direction of the company changes. In some cases, a strategic change in a company's direction may mean the cancellation of some projects and the creation of new ones.

There have been many instances where senior executives see BCM as a project to be completed in a specific timeframe, usually a short one. Once it's completed and the multiple binders have been formatted and printed, it's forgotten and placed on a shelf beside other binders no one reviews, collecting dust. BCM is never a project, that's why it's called a BCM program. By definition, a project has a start and end date with defined deliverables. Since BCM is meant to mirror an organization, it's hard to call it a project when the organization is in constant change in one form or another. To keep BCM current, it must be living and breathing and walking with the rest of the organization as it changes.

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) Explain briefly the BCM audit process.

.....

.....

.....

.....

2) What is the role of BCM audit process and explain its key functions?

.....

.....

.....

.....

3) What are key considerations in BCM audit?

.....

.....

.....

.....

4) What are BCM audit's concerns and focus?

.....

.....

.....

.....

5) What are most common BCM weaknesses?

.....

.....

.....

.....

2.8 FUTURE OF BCM

Deeper, not Broader

Most importantly, it's not clear that the best strategy out of the profession's conundrum is to try to establish its value by branching out horizontally. Someone is asking the business continuity professional to justify her value on grounds that she can do someone else's job, but this opens her up to the reply "that's great, but we already have someone else doing those jobs."

It's normally not prudent to stake your value on grounds you can do someone else's job. Rather, it's best to demonstrate that only you can do your own job. The medical profession did not establish its importance by encouraging doctors to add plumbing to their skill-set. They demonstrated their value by demonstrating that they had knowledge of medicine beyond that of anyone else.

In other words, the business continuity profession is better served by deepening, rather than broadening, his or her knowledge. Any profession is better served by cutting a unique niche that is not in other's competency, than by attempting to insert oneself into another's business.

The profession needs research to legitimate itself and establish its value. Too much of business continuity practice is intuition driven, rather than evidence driven. While it certainly makes intuitive sense that organizations with a business continuity plan will fare better than one without a plan during a disaster, has that ever been tested and proven? Many people quote a statistic, which varies according to the author that "X" percent of companies without a business continuity plan fail after a disaster.

But as someone points out, even if true – and it turns out that it is hard to track these statistics back to a reliable origin – that would not tell us anything about

the value of such plans until we compare the survival rates of companies with a business continuity plan to those without a plan. It might be the case that companies without a business continuity plan fare just as well as those with one.

Of course, I personally believe that having a business continuity plan is better than not having one, but convincing a skeptical upper management of this fact is going to require more than my asserting – in pretty forceful and unambiguous terms – that I think it's true.

The problem is that studies up to now lack the foundational scientific principle of a control group. Without a control group very little can be concluded from a study. Until the late 1800's, doctors were using the accepted practice of bloodletting to treat most diseases. In the world view of the time, it made more intuitive sense to think that disease was caused by bad spirits than the new-fangled theory of "germs" so small you couldn't see them. It wasn't until someone actually compared the recovery rates of those who were treated with bloodletting to those who were not treated with this practice they discovered, much to their surprise, that bloodletting did not actually make recovery more likely. Who would have guessed?

A while ago people predicted that insurance companies would require companies to have business continuity plans. This has not materialized because insurance companies are driven by actuarial tables – evidence of loss based on different factors. There is simply no evidence that business continuity plans lower loss. Again, I think (or hope) they do, but that's not enough to convince the insurance companies.

The business continuity profession needs to deepen, rather than broaden, its knowledge base to establish its value. This means comparing the results of different business continuity techniques. For instance, there is currently a debate in some circles over whether a risk analysis should come before or after a BIA. Has anybody compared the two methods to determine which yields better results?

Research will also help produce a common set of definitions, which is sorely needed in the profession, and a common body of knowledge. Note that a common body of knowledge does not mean that everyone is forced to accept principles without question. Quite the opposite. Scientific progress can only be made when there is an accepted way of doing things that can be subjected to rigorous testing against alternatives. In other words, a common body of knowledge serves as a foundation against which people can test new ideas.

Right now too many commentators act as if they were the first person to have ever spoken on their chosen topic. There is very little sense of challenging, or adding to, a common understanding in most business continuity articles. The profession carries the air of a variety of commentators with different

perspectives, rather than an organized development of knowledge. While it might sound combative, and unfortunately research can become that, knowledge can only advance when one researcher argues for or against the results of others.

Colleges and universities are in the process of fostering research to advance the field. The goal is to provide more of an organized structure to research into the field so that it advances in a way that builds up prior understanding. Some of this research will undoubtedly support commonly held beliefs, thus providing credence to what professionals are already doing. That is important to moving the field forward. But much of the research will likely challenge current orthodox.

These counter-intuitive results will be the most interesting and possibly the most important to a field. A business continuity professional who can say to a prospective employer "while it might seem the practice you are doing is best for the organization, research actually demonstrates that this other practice generates better results in the long run." That person presents themselves as having knowledge that others do not have precisely because it is not intuitively obvious.

Someone may have accurately painted a gloomy view of the business continuity professional's life – though I'm sure many people will disagree. We all want to elevate the profession's status, but the light at the end of the tunnel is more likely to be found by deepening, rather than broadening, the profession's knowledge. To be clear, it is important for the business continuity professional to have an understanding of periphery fields to do his or her job well. But the profession will only establish its value by pursuing a deeper understanding of the business continuity practice.

2.9 LET US SUM UP

BCM is an important risk management program designed to protect companies from potential significant consequences related to events that can disrupt critical business processes. The auditing and evaluating of BCM program can help the organization understand the risks and the options to create an effective BCM program. Managers throughout the organization must be held accountable for appropriately managing the risks associated with disruption of the business operations and associated functions within their organization. A BCM program provides the framework for making appropriate risk mitigation decisions and building organization resilience. Critical business processes must be recovered to support the recovery of critical business operations. The BCM program enables an organization to maintain recovery capabilities, including organizational capabilities and knowledge, systems and information recovery, resource restoration and procurement, supplier management, and alignment

with emergency Management processes. The BCM program should be designed to maintain and grow the business continuity capabilities continuously. Effective maintenance of the BCM capabilities must include regular training of staff, periodic exercises (including resolution of any identified gaps and management commitment to the program), audit assessments of the BCM program and business unit capabilities and continual improvement of the BCM program.

2.10 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

1) Business continuity management is the process by which an organization prepares for future incidents that could jeopardize the organization's core mission and its long-term viability. Such incidents include local events like building fires, regional events like earthquakes, or national events like pandemic illnesses.

   The key components of the BCM are:

   - Management Support
   - Risk Assessment and Risk Mitigation
   - Business Impact Analysis (BIA)
   - Business Recovery and Continuity Strategy
   - Awareness and Training
   - Exercises
   - Maintenance

2) There are several types of auditors such as internal auditors, external auditors, and compliance auditors.

   - Internal auditors are employees of a company that assess and evaluate its systems of internal control. A business continuity plan is considered to be an important component of an internal control system. To maintain independence, they present their reports directly to the board of directors or to executive management.
   - External auditors are independent staff of an auditing firm that assess and evaluate financial statements of their clients or perform other agreed upon evaluations such as IT Audits that may also address the business continuity plans of the organization.
   - Compliance auditors are examiners normally from a regulatory agency such as FFIEC, FERC, DHS/FEMA, JCAHO/HIPAA and others depending on the type of industry.

3) The audit may be prompted by the internal audit department, external audit organization such as the CPA firm that performs the financial audit, or a regulatory examiner. Another reason is it may be triggered by the results of an emergency event or by the results of a test exercise. Board and/or executive management may also request an audit of the business continuity management program or components thereof. In some cases a customer may request a BCM audit such as customers of service organizations.

4) The BCM audit provides an independent evaluation of the BCM program and identification of strengths and weakness of the program. The audit can also reveal high risks and associated mitigation strategies. The results should include recommendations for BCM improvements and identification of "best BCM practices." Other benefits are:

   - Objective evaluation of the BCM Program
   - Business continuity office
   - Internal and independent
   - External and independent
   - Alignment with other similar organizations
   - Demonstrate compliance and diligence

5) There are several BCM standards, guidelines and frameworks that are used for developing BCM plans including:

   - Disaster Recovery Institute International (DRII)
   - Business Continuity Institute (BCI)
   - COBIT – Control Objectives for Information and Related Technology
   - ISO 17799/27000 Series
   - National Fire Protection Association 1600 (NFPA 1600)
   - BS 25999 (British Standards Institute)
   - Various state statutes and regulatory requirements

6) The most general definition of an audit is an evaluation of a person, organization, system, process, project, or product. A BCM audit is an independent evaluation of the business continuity management program or its components by internal or external independent parties. The organizations top management should, at intervals that it deems appropriate, review the organizations BCM capability, to ensure its continuing suitability, adequacy and effectiveness. This review should be documented and can take the form of:-

   1. Internal audits
   2. External audits
   3. Self Assessments

Check Your Progress 2

1) The BCM audit process includes

- an audit plan
- The BCM Assurance process
- Methods and Techniques
- Outcomes and Deliverables
- Review

2) The BCM audit process plays a key role in ensuring that an organization has a robust, effective and fit-for-purpose BCM competence and capability. It has five key functions:

1. to independently verify compliance with the organization's BCM policy, strategies, framework and good practice guidelines or standards adopted by the organization.
2. to independently review the organization's BCM solutions.
3. to independently verify and validate the organization's BCP and crisis management procedures.
4. to independently verify and validate that key exercising and maintenance activities are taking place, in line with the relevant programmes, processes and the organization's BCM framework.
5. to highlight key material deficiencies and issues and ensure their resolution.

3) The following key considerations should be applied to it:-

a. The role and perspective of the auditor and audit function is one of impartial review against defined standards. Whilst the auditor may be fully aware of and may identify the reasons for BCM shortcomings and organizational difficulties, the auditor should clearly identify the BCM competence and capability gaps.

b. An integral part of the audit is to provide remedial recommendations.

c. Each stage of the BCM life-cycle may require a different audit approach. The audit approach is solely dependent upon the maturity of each stage of the BCM life-cycle.

d. A proactive audit process should be seen as an enabling process to achieve a particular management objective.

e. The audit process can be undertaken by an organization's internal audit function, an external auditor, or external professional BCM practitioner. The scope of the audit should be material to the organization, clearly defined, documented and agreed in partnership with the relevant auditee

and senior management. Where auditors do not have the requisite professional level of BCM knowledge, expertise and experience, they should employ the assistance of a professional BCM practitioner.

4. BCM Auditors may have several concerns related to the BCM as described below :-

   - Risk Assessment – The BCM auditor may audit the results of the risk assessment as well as the process that was used during the development of the risk assessment to understand if it was comprehensive.

   - Business Impact Analysis – The BCM auditor may audit the results of the business impact analysis as well as the process that was used during the development of the business impact analysis to understand if it was comprehensive.

   - BCM Structure and Documentation – Effective documentation and procedures are extremely important in a business continuity plan. Considerable effort and time are necessary to develop a plan. However, many plans are difficult to use and become outdated quickly. Poorly written procedures can be extremely frustrating.

   The BCM auditor may audit the BCM structure and documentation. The audit may review activation procedures, communications plan, recovery teams, scenarios, command and control center, alternate facilities, detailed recovery procedures, and other considerations.

5) Some common weaknesses of business continuity plans identified as a result of BCM audits are listed below:

   - Often there may be a BCM plan but it may not contain a BCM policy statement.

   - Organizations often have multiple types of plans without adequate integration. For example the emergency plan or the crisis management plan may not be properly coordinated with the BCM. This can result in confusion at the time the plan(s) need to be activated.

   - Some organizations have developed comprehensive business continuity plans, but maintenance roles and responsibilities have not been clearly defined. This can result in the BCM quickly becoming outdated.

   - There may be a lack of training and knowledge transfer of the BCM. This creates a significant reliance on a few individuals and can result in improper execution of the plan.

   - Many organizations perform IT testing exercises but limited testing in other areas. This also can create problems if the plan needs to be activated.

- In some organizations, the IT professions develop the BIA and determine priorities without stakeholder involvement. Although IT professionals often have a good understanding of the business processes, a lack of stakeholder involvement can result in incorrect RPOs and RTOs.
- Many organizations do not include BCM in the change management process. This can result in the system being implemented without a recovery strategy.
- Some organizations have developed good recovery strategies but have not documented the procedures to support their strategies.

2.11 SUGGESTED READINGS

- Auditing Business Continuity: Global Best Practices By Rolf von Roessing
- http://public.pacbell.net/faq/general_faq.htmlhttps://www.issatr.org/wp-content/themes/issa/images/ISSA-JUNE2010bcm-FINAL.pdf
- http://www.bcmpedia.org/
- The Definitive Handbook of Business Continuity Management By Andrew Hiles.

UNIT 3 DEVELOPING AND IMPLEMENTING A BCM RESPONSE

Structure

3.0 INTRODUCTION

Determining and Implementing a BCM response is key to success or failure of a BCM programme. It covers the development of an appropriate detailed action plans in order to ensure continuity of activities or recovery of critical activities and thereby effective incident management.

The aim of the various plans is to identify the critical activities, evaluate the threats to these critical activities ,choose appropriate plans to reduce the likelihood and impact of incidents so that the organization is able to manage an interruption whatever its cause and thereby safeguards the interests of its key stakeholders, reputation, brand and value creating activities.

The main requirements for an effective response are:

- A clear procedure for the escalation and the control of an incident (incident response structure)
- Communication with the stakeholders
- Plans in order to resume interrupted activities

The actions that are outlined in plans are not intended to cover every eventually as, by their nature, all incidents are different. Any predefined procedures may need to be adapted with flexibility and initiative by those responsible for implementing the plan to the specific event that has occurred and the opportunities it may have opened up.

3.1 OBJECTIVES

After studying this unit, you should be able to:

- know the contents of Plan;
- explain Incident Response Structure;
- explain Incident Management Plan; and
- know the Operational Response Plan.

3.2 INCIDENT

An Incident is defined as any unplanned event that has the potential to significantly affect the well-being of organization members, its image or operations, or to pose a significant economic or legal liability.

3.2.1 Criteria for Evaluating

- Fatalities and serious injuries caused by either "acts of God" or other causes, e.g., suicide, assault, robberies, traffic accidents, etc.
- Significant environmental damage e.g., floods, fires, etc.
- Any other event or incident that poses potential damage to the organization reputation or credibility, e.g., discovery of misuse of organization funds, etc.

Incidents that do not meet these "significance" criteria stated above will not be managed with the incident management process, but will be handled in the routine course of business.

3.2.2 Classification

Incidents can have different dimensions depending upon there geographical impact, there potential for harm to human health and the environment or their economic or image impact to the organisation. For ease of differentiation, the following classification system is used:

Class III Incident: A catastrophic emergency event involving the entire organization and surrounding community or a major incident with national implications. The potential public and environmental exposure is truly significant. Maximum organization and third-party resources should be used to control and correct the problem. Governmental involvement and media interest will be intense. For example:

A major release of toxic chemicals caused by a fire releasing emissions over the organization and the City of Flagstaff.

Class II Incident: A major emergency that impacts a sizeable portion of the organization or outside community or an incident with at least regional implications. The potential public and environmental exposure is of significant concern. Local organization resources may have to be supplemented with third-party resources to manage the event. Public and media interest will be moderately high but primarily at the local and regional level. For example: A major fire at one of the organization's office that results in minor injuries and staff evacuation.

Class I Incident: An incident with state and local implications. The potential public and environmental exposure is minimal. For the most part, the problem can be corrected with local resources and some third-party resources. Public and media interest will be moderately high but restricted primarily at local levels. An example would be the disclosure of one of the organization's t heads involved in misallocating the organization's funds for personal use.

3.2.3 Incident Response Structure

In any incident situation there should be a simple and quickly formed structure that will enable the organization to:

- Confirm the nature and the extent of the incident
- Take control of the situation
- Contain the incident and
- Communicate with stake holders

An organization should define an incident response structure which may be referred as the incident management team (IMT) or crisis management team (CMT).The team should have plans, process and procedures to manage the incident which should be supported by business continuity tools to enable continuity and recovery of critical activities. The team should have plans for the activation, operation, coordination and communication of the incident response.

One model of incident response of the UK Emergency Services, shows three tires of incident response referred as Gold, Silver and Bronze. When applied to an organisation's response structure the responsibilities are as follows.

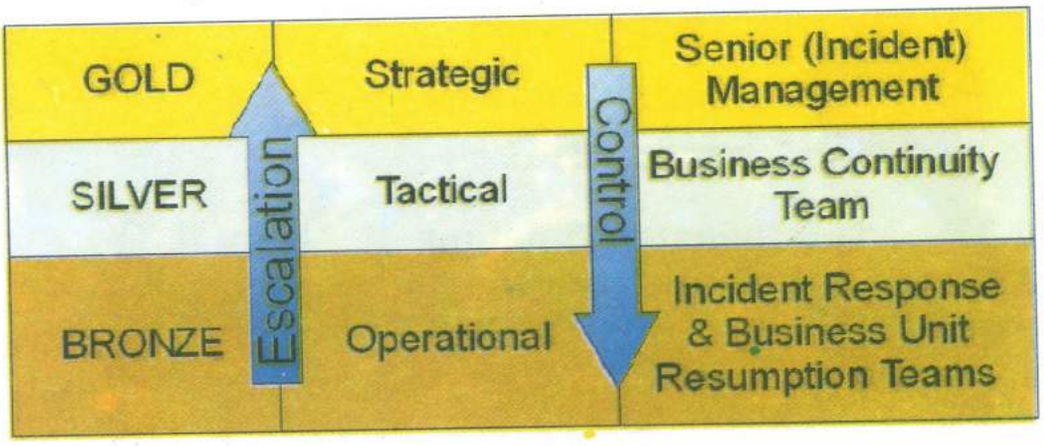

Fig.1

Strategic Level - Incident Management Plan (IM

This plan details how the incident will be managed from the occurrence to back-to-normal operation and provides the information about the structure of the Incident Management Team, the criteria for invoking Business Continuity, the management of the incident, resource requirements, any necessary staff movements and critical processes.. This may be when the incident is not entirely the scope of the Business Continuity Plan. The Incident Management Plan is sometimes known as 'Crisis Management Plan'.

Tactical Level: Business Continuity Plan (BCP)

The BCPs address business disruption, interruption or loss from the initial response to which the normal business operations are resumed. They are based upon the agreed Continuity Strategies and provide the procedures and the processes for both the business continuity resource recovery teams. In particular the plans allocate the roles and their accountability,responsibility and authority. The plans must also detail the interfaces and the principles dealing with a number of external players in the response.

If the event lies outside the scope of the assumptions on which the Business Continuity was based then the situation should be escalated to those responsible for implementing Incident Management Plan (IMP).

Operational Level: Activity Resumption Plans

The plans provides resumption of normal business for operational departments such as Facilities and IT that are managing infrastructure.It will provide a structure for restoring existing services or provide alternative facilities.

3.2.4 Incident Timeline

There are three main phases over time of an incident, and the relationship between incident management and business continuity.

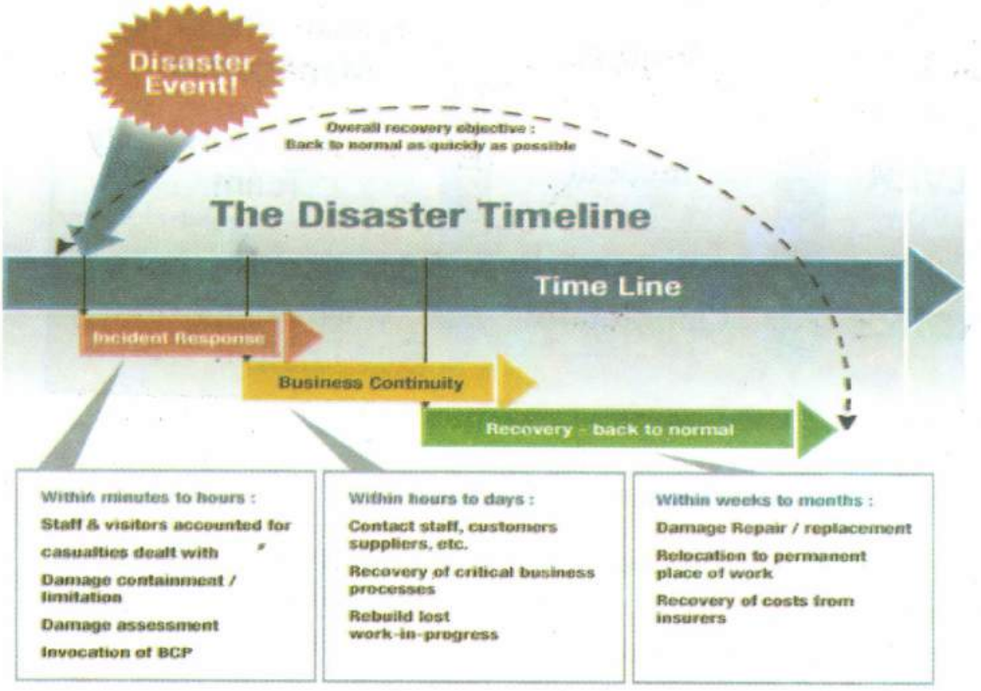

Fig.2

The three phases of an incident, as shown in figure:

- **Response**: to an incident, emergency or disaster;
- **Business Continuity:** business-critical activities (this may include interim workarounds in the absence of essential technology);
- **Recovery:** normal working of all business operations from the temporary measures adopted during recovery.

The Organization may develop specific plans to recover or resume operations back to a "normal" state (recovery plans). However, in some cases it might not be possible to define what "normal" looks like until some time after the incident, so it might not be possible to implement the recovery plans immediately.

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 BCM response does?

.....

.....

.....

.....

2) In how many class the incident is classified?

.....

.....

.....

.....

3) Name the levels presented in incident response structure.

.....

.....

.....

.....

3.3 CONTENT OF PLANS

All plans, whether it is incident management plans, business continuity plans or action response plans, should be concise and accessible to those with responsibilities defined in the plans.

3.3.1 Purpose and Scope

Each plan should set out prioritized objectives in terms of:

- The critical activities that should be recovered;
- The timescales in which they are to be recovered;
- The recovery levels needed for each critical activity;
- The situation in which each plan can be utilized.

3.3.2 Roles and Responsibilities

- The roles and responsibility of the people and the teams having authority during and following an incident should be clearly documented.
- The persons or the groups covered by a plan should be clearly defined.

3.3.3 Plan Invocation

The invocation process may require the immediate draft of organizational resources. The plan should include a clear and specific description of:

- How to mobilize the team(s);
- immediate rendezvous points; and
- Following in order team meeting locations and details of any alternative meeting locations

3.3.4 Document Owner and Maintainer

- The organization should appoint the primary owner of the plan, and identify and document who is responsible for reviewing, amending and updating the plan at regular intervals.
- A system of version control should be employed, and changes should be formally notified to all interested parties with a formal plan distribution and it should be recorded, maintained and kept up-to-date

3.3.5 Contact Information

Each plan should contain or provide a reference to the essential contact details for all key stakeholders.

3.4 INCIDENT MANAGEMENT PLAN

3.4.1 Introduction

The important factor in protecting an organization's brand from financial and reputation damage depends on how effectively and rapidly the crisis is managed.

The Incident Management Plan (IMP) may be the first element to develop for organisations with no plans in place thereby providing a limited amount of protection while other plans are developed. It is important that an organisation chooses names (IMT/CM or response team) that fit into its culture and structure. Some incidents will require an IMT response even though they are not a result from disruption to activities for example those involving threats to reputation alone does not involve a Business Continuity response. However, there is always a need to involve the IMT where a BC response is required just to make them aware of the situation in case it escalates.

3.4.2 Purpose

The purpose of an IMP is to provide a documented framework to enable an organisation to manage all possible issues, including the stakeholder and external issues, facing the organization during an incident regardless of cause (including those where no Business Continuity response is appropriate such as a threat to reputation).

3.4.3 Process

In outline the IMP should:

- Assign an owner for the Plan on the Executive
- Describe the objectives and scope of the plan

- Build up and approve a Incident Management plan development process and programme
- Form an Incident management planning team to develop the plan which should be modular in design
- Have a claims management procedure that ensures all insurance and legal claims for or against the organization meet regulatory and contractual requirements
- Agree the tasks of the Incident Management Team and their relationship with other plans
- Decide the structure, the format, the components and the content of the plan
- Establish the strategies, for instance alternative locations, on which the plan is based
- Collect information to populate the plan
- Appoint individuals and deputies (if the senior management team is too large)
- Appoint administrative support for the IMT
- Draft the plan
- Be supported by an appropriate budget for development, maintenance and training
- Pass the draft of the plan for consultation and review
- Collect feedback from the consultation
- Modify plan as appropriate
- Agree and authenticate the plan, for example by using it in an exercise
- Do again the process for the Incident Communications Plan (if separate)
- Consent a programme for continuing exercising and maintenance of the plan to ensure it remains current

3.4.4 Methods and Techniques

The Incident Management Plan structure

The methods, tools and techniques used in the planning and development of an Incident

Management Plan includes:

- Stakeholder analysis
- Scenario planning

- Checklist(s)
- Workshops

A range of software products are available to aid in building and maintaining a Incident Management Plan. These can provide significant benefits in areas of the maintenance of the plan and its referential integrity but these are not necessary and do not replace knowledge of the business.

3.4.5 IMP Contents

It is a set of components and resources that may be useful to the team tasked with activating the plan. The contents depend on the nature and complexity of the organization and the nature of the crisis.

3.4.5.1 Roles and Responsibilities

The roles of the team and particular individuals should be documented. Deputies should be known for each role. Only **incident** roles should be used throughout the document and not names. Responsibilities for the team or nominated individuals may include:

- Managing communications
- Ensuring IMT and BCT are correctly staffed and make appointments if necessary
- Liaising with the Business Continuity Team to consent resumption timetable
- Approving important expenditure
- Monitoring the overall growth of recovery and personnel performance
- Identifying and maximizing opportunities or advantages arising from the incident
- Looking at the strategic impact of the incident on the organisation - which may require major changes in direction or open up new opportunities
- Maintaining a decision log during the incident.

3.4.5.2 Invocation Instructions

Document the circumstances in which the team will be activated and the persons responsible to initiate the call-out should be decided. Due to the nature of incidents, some flexibility and encourage action should be allowed since it is easier to stand down activated team than activate them after the incident has developed out of control. The way by which the team will be activated should be documented so that decisions can make in the shortest possible time. On

invocation the first notified should recognize most suitable meeting place and a fallback, based on the current information.

3.4.5.3 Action plans

The plan should contain first prompts for action such as stakeholder list. The Business Impact Analysis may enclose useful pointers to possible impacts that will need to be managed. It is helpful if these are included as a checklist and have a box for ticking that the action has been accomplished. At times it is useful if action checklists are written for each member of the team separately so they can be printed and handed to each individual

3.4.5.4 Incident Management Location

A robust and predetermined location, room or space from which an incident will be managed should be defined by the organization. At least two locations should be chosen to act as an incident management centre (control room or command centre). One should be on-site where the senior management team is based and the other should be designated off-site. It is not necessary for the organization to own the off site location. By prior arrangement, 24-hour hotel should be able to deliver all the facilities required for most of the organizations.

The chosen location should be fit-for-purpose and include:

- the layout of the room
- details about catering arrangements
- shift lengths
- effective primary and secondary means of communication;
- facilities for accessing and sharing information, including the monitoring of the news media;
- controlled entry

If the room is normally a meeting room it is sometimes useful to prepare a notice for the door, stating that in the case of an incident the room must be vacated at once.

3.4.5.5 Resources

The following resources should be included:

- Whiteboard/flip charts (and pens that work)
- A number of telephones together with at least one ex-directory outgoing line phone recording facility
- Helpline facility

- Cell phones, fax, e-Mail and Internet
- TV and radio monitoring equipment
- Videoconferencing
- Stationery
- A means of logging all actions.
    - Details of equipment storage and staging areas
    - Site access plans
- Refreshments and nearby or on-site sleeping facilities
- A separate and nearby location for hosting the press

Hardware and information can be kept off-site at the alternative location in a locked trunk (Often called a 'battle-box' or 'recovery box').

3.4.5.6 Task and Action List

The IMP should include task lists and action checklists to handle the immediate consequences of a business disruption. These tasks should:

- ensure that safety of individuals is addressed first;
- be based upon the results of the organization's BIA;
- be structured in a way that delivers the strategic and tactical options chosen by the organization,
- help prevent the further loss or unavailability of critical activities, and supporting resources

During planning special needs of individuals during evacuations or stay-in periods like pregnancy, disabilities and family responsibilities should be included.

During an incident the IMP should identify the person(s), who will discharge responsibility for welfare issues including:

- Site evacuation (inclusive of internal "shelter-at-site" activities);
- Accounting for the staff, the contractors and the visitors
- Communicating with staff and others on the site or in the immediate vicinity
- The mobilization of safety, first aid
- Setting up a staff help line

Later there may be additional needs like:

- Temporary accommodation
- Counselling and the rehabilitation services which could be provided as part of an employee health package

Welfare needs at alternative locations like:

- Refreshments
- Personal safety and security
- Transport and accessibility
- Appropriate training on replacement equipment
- Special needs

3.4.5.7 Emergency Services Liaison

The organization will correspond with staff and their relatives, friends and emergency contacts should be included. In some cases, it might be right to include detail in a separate document. Next-of-kin and emergency contact information for all personnel should be kept up-to-date and available for prompt use.

Staff with a suitable level of experience and authority should be chosen to liaise with the emergency services at the arrival on site and subsequently as required. The emergency services should be given information on the location of any victims and the status of the condition and any known hazards they may encounter.

At the same time on the site, the emergency services instructions take priority over those given by the organization's own staff. On departure from the site, the organization will carry on responsibility for its own site security.

3.4.5.8 Media Response

The media response should be documented in the IMP, including:

- the incident communications policy;
- the organization's number one interface with the media (eg. local or national newspapers or radio or TV or internet or other media)
- a guideline or template for the drafting of a statement to be provided to the media at the first practicable opportunity following the incident;
- appropriate numbers of trained, competent, spokespeople designated and authorized to release information to the media;

- establishment, where practicable, of a suitable location to support liaison with the media, or other stakeholder groups.

In some cases, it may be suitable to:

- provide supporting detail in a separate document;
- establish a proper number of competent, trained people to answer telephone enquiries from the press;
- prepare background material about the organization and its operations ;
- make sure that all media information is made available without unnecessary wait

3.4.5.9 Stakeholder Management

It is important to maintain a separate stakeholder management plan to provide criteria for setting priorities and allocating a person to each stakeholder or group of stakeholders. It should address how the organisation will manage communication with all stakeholders including:

- Staff, relatives, friends and emergency contacts
- Customers and suppliers
- Shareholders or owners
- (If part of a group or larger organisation) liaising with other members of the group or head office
- Informing and liaising with regulatory authorities
- Dealing with matter related to serious injuries or fatalities (having discussion with the emergency Services and in accordance with local regulations and customs)
- Media

In advance following things should be taken care of:

- What crises could hit us?
- Who are the audiences?
- How can we correspond with them?
- What are the Messages?
- Who will form the Incident Team?
- What are the Resources and Facilities?
- Are the Incident team and spokespeople trained?
- Does it Work?

- What Incident Manual do we need?
- Have we built lines of communication with our audiences?
- When a crisis or business discontinuity gets into the public domain, helpful communication will play a important role in rescuing and maintaining an organisation's most valuable asset - its reputation.

When crisis are faced consider:

- Plan ownership: all those who have to take decisions about how to communicate must have agreed beforehand on the who, how and what to communicate.
- Reality of the perception: the reputation is not affected so much by what has happened but as by what people think has happened and by their perceptions of how it will be handled.
- Understand the key audiences and what they want to hear.
- Act fast: With every passing hour of silence the reputation problem doubles. So the organization needs to seize the communications on high ground.
- Be open: give that much of information to various audiences as legally and practically the organization can there by showing there is nothing to hide which helps to allay suspicion.
- Show you care: The content of the message should be what the audience wants to hear **Resources**

3.4.6 Review

The review or audit should be associated with the review of other BCM and Incident Management related strategies, plans and solutions.

It should be initiated by a major business or senior management change or important change in the external operating environment.

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 role of the document owner and maintainer?

.....

.....

.....

.....

2) What is the need of a modular design?

.....

.....

.....

.....

3) How many incident room should be chosen and where they should be located?

.....

.....

.....

.....

4) Which box is called recovery box?

.....

.....

.....

.....

5) What are the special needs of individuals during evacuation?

.....

.....

.....

.....

3.5 BUSINESS CONTINUITY PLAN

3.5.1 Introduction

The Business Continuity Plan takes care how to stay in business at the occurrence of a disruptive incident by facilitating the resumption of business activities. This plan will help in analyzing information from the response teams concerning the impact of the incident, selecting and deploying appropriate strategies available, direct the resumption of business units according to decided priorities and pass progress information to the Incident Management Team.

This plan will vary from organisation to organisation in reference to its components and content and will have a different level of detail based on the culture of the organization and the technical complexity of the solutions.

3.5.2 Purpose

It provides a documented framework and process so that the organisations can resume all of its business processes within their RTO. This Plan alone does not demonstrate a BCM competence or capability. BCPs are activated (invoked) to support the critical activities which are required to deliver the organization's objectives

3.5.3 Process

In outline the BCP should:

- Select an owner (or each plan for multiple sites)
- Action orientated
- State the objectives and scope of the BCP with reference to the organisational strategy and BCM Policy
- Build up and agree a planning process and timetable programme
- Build a planning team to carry out the plan development
- Decide the structure, the format, the components and the content of the plan
- Find out the strategies which the plan will document and what will be documented in other plans
- Determine the conditions that are beyond the scope of the BCP
- Collect information to populate the plan
- Modular design
- Draft the plan
- Pass the draft of the plan for consultation and review
- Group feedback from consultation process
- Modify the plan as appropriate.
- List ongoing exercising and maintenance of the plan to establish it remains current
- Test the plan using a desktop exercise

3.5.4 Methods and Techniques

A number of software products are existing to aid in building and maintaining a Business Continuity Plan however it is not essential. The normal office software (Word processor and spreadsheet) is sufficient and is more inclusive of all staff as its use does not require any special training. Customized software

can however provide remarkable benefits in the areas of plan maintenance and referential integrity.

There must be a clearly defined and documented control and change management process for the production, the update and the distribution of the Business

3.5.5 BCP Contents

It is a set of components and resources that may be useful to the team tasked with activating the plan. The content depends on the nature and complexity of the organization and the nature of the crisis.

3.5.5.1 Roles and Responsibilities

The roles of the team and definite individuals should be documented. Deputies should be identified for each role. Responsibilities of the team or specific individuals may include:

- Liaising with the Emergency Services
- Receiving or seeking information from response teams
- Reporting information to the Incident Management Team
- Mobilising third-party suppliers of salvage and recovery services
- Allocating available resources to recovery teams

3.5.5.2 Invocation Instructions

Document the circumstances in which the team will be activated and the persons responsible to initiate the call-out should be decided. Due to the nature of incidents, some flexibility and encourage action should be allowed since it is easier to stand down activated team than activate them after the incident has developed out of control. The way by which the team will be activated should be documented so that decisions can make in the shortest possible time. On invocation the first notified should recognize most suitable meeting place and a fallback, based on the current information.

3.5.5.3 Action Plans / Task List

The action plan should include a planned checklist of actions and tasks in an order of priority, highlighting:

- How the BCP is invoked
- The person(s) responsible for invoking the business continuity plan;
- The procedure that person should agree to in taking that decision;
- The person(s) who should be consulted before such a decision is taken;
- The person(s) who should be intimated once a decision has been taken;

- Who goes where, and when;
- What services are available where, and when; including how the organization mobilizes external and third-party resources;
- How and when this information is communicated;
- If relevant, full procedures for manual workarounds, system recovery, etc.
- Initiate activity recovery
- Receive information from other teams
- Report status to Incident Management team

3.5.5.4 Resource requirements

The resources needed for business continuity and business recovery should be recognized at different points in time.

a) **People, which may include:**

- security,
- transportation logistics,
- welfare needs, and
- emergency expenses;

b) **Premises;**

c) **Technology, including communications;**

d) **Information, which may include:**

- financial (e.g. payroll) details,
- customer account records,
- supplier and stakeholder details,
- legal documents (e.g. contracts, insurance policies, title deeds, etc.),
- other services documents (e.g. service level agreements);

e) **Supplies;**

f) **Management of, and communication with, stakeholders.**

3.5.5.5 Responsible Person

The organization should recognize a nominated person to handle the business continuity and business recovery phases of a disruption.

3.5.5.6 Forms

The business continuity plan should comprise of an incident log or forms for the recording of very important information, especially in respect of decisions made.

3.5.6 Review

Some information such as contact details should be reviewed in line with BC policy. Other information should be officially reviewed annually and tested through exercising. Other triggers leading to a review are:

- An important change in the technology or telecommunications

There is a big business process change

- A significant change in staff
- A change in the supplier of BC solutions

Check Your Progress 3

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

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

1) What are the responsibilities of the team or the specific individual in BCP?

.....

.....

.....

.....

2) What is considered as vital information in BCP?

.....

.....

.....

.....

3) What leads to major business process change?

.....

.....

.....

.....

3.6 OPERATIONAL RESPONSE PLAN

3.6.1 Introduction

This plan covers the response by each department or business unit to the incident. Examples are:

- The procedures to help an incident response team generally lead by a Facilities department who deal with the definite incident and its physical impact
- A Human Resources response to welfare issues
- A business department plan to resume its functions within a predefined timescale
- An IT department's logistical response to the loss and following resumption of IT services to the business

The complexity and urgency of the business processes may decide whether one operational plans covers a single activity or a department covering several activities. The operational response plans depending on the complexity of the organization may be supported by more detailed plans for specific responses, locations or equipment.

3.6.2 Purpose

The purpose is to organise the response of each department to a disruption within the overall Business Continuity Plan.

3.6.3 Process

The outline of the Business Unit Resumption Plan development and planning process include:

- Assign a person to be responsible for development of the plans overall and a representative within each operational unit to develop their plan
- Define the objective and scope of the plans
- Build up a planning process and timetabled programme. Where possible, begin with the plans for the most vital business activities
- Decide the overall BCM strategies on which the plan is based.
- Decide the structure, the format, the components and the content of the plans
- Build up an outline or template plan to encourage standardization of documentation but allow individual variations where this is appropriate

- Ensure that Business Units appoint individuals to fulfill roles within their plans
- Manage and mentor the development of plans within the Business Units
- Pass the draft of the plan for consultation, review and challenge within and, where necessary outside, the department
- Collect feedback from consultation
- Alter plan as appropriate
- Authenticate the plan through a unit test
- Consolidate the BU plans and review for uniformity
- Document connections with the BC Plan and between Unit plans
- Does resource requirements analysis across all plans to define resource for support functions

3.6.4 Methods and Techniques

The methods, tools and techniques to build up an Operational Response Plan comprises of:

- Interviews (structured and unstructured)
- A Business Impact Analysis and Resource Requirements analysis for this activity
- Checklists and templates
- Workshops

Specific Response plans may include the following:

- Facilities (Incident Response Team)
- Staff Welfare plans
- Business Unit Resumption
- IT Disaster Recovery

The above plans may include suitable procedures and information such as:

- Building Evacuation and "Stay-in" plans
- Response to Bomb Threat and similar scenarios
- Evacuation Points (including alternate or off-site)
- Emergency Services Liaison

- Dispersal of staff and visitors
- Salvage Resources and Contracted Assistance
- Escalation circumstances
- Human Resource and Welfare issues
- Health and Safety legal liabilities
- Procedure for accounting for staff
- Procedure for contacting staff
- Counselling and rehabilitation resources
- Escalation criteria
- Escalation procedure to Business Continuity Team (BCT)
- Response to Initial contact from BCT
- Contacting team members
- Resumption Plan for each process
  - Staff numbers
  - Key contacts
  - Procedure for resumption of business activity
  - Activity Priorities
  - Special procedures
  - Work in Progress issues
  - Consumables required

3.6.5 Review

Operational Response plans should be reviewed if there is a key change in the business process or technology within that area.

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) Why the design should be action orientated?

.....

.....

.....

.....

2) What are the outcomes of the operational response?

.....

.....

.....

.....

3) When should the operational response plan be reviewed?

.....

.....

.....

.....

3.7 LET US SUM UP

Developing and Implementing a BCM Response includes:

a) Developing and implementing crisis response actions for responding to and stabilizing the situation following an incident or event.

b) Establishing and running an Emergency Operations Center to be used as a command center during the crisis.

c) Practical experience in handling incidents/emergencies

d) Designing, developing and implementing plans that provide continuity within recovery time and/or recovery point objectives.

3.8 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

1) BCM response mainly focuses on the immediate drills and steps taken shortly after an incident or disaster.

2) In three classes the incident is classified.

3) Three levels are presented in Incident response structure namely strategic level, tactical level and operational level.

Check Your Progress 2

1) The role of the document owner and maintainer is:

- The organization should appoint the primary owner of the plan, and identify and document who is responsible for reviewing, amending and updating the plan at regular intervals.
- A system of version control should be employed, and changes should be formally notified to all interested parties with a formal plan distribution and it should be recorded, maintained and kept up-to-date

2) The plan should be in modular design so that single sections can be supplied to individuals or team on a need to know basis.

3) Two incident room should be chosen. One should be at on-site and other should be designated off site.

4) Hardware and information kept off site at the alternative location in a locked trunk is known as recovery box.

5) The special need of individuals during evacuation is pregnancy, disabilities and family responsibilities.

Check Your Progress 3

1) The Responsibilities of the team or specific individuals may include:
   - Liaising with the Emergency Services
   - Receiving or seeking information from response teams
   - Reporting information to the Incident Management Team
   - Mobilizing third-party suppliers of salvage and recovery services
   - Allocating available resources to recovery teams

2) The vital information in BCP is customer information, contact details, legal documents and service level agreement.

3) When there is significant change in staff and in the supplier of BC solutions then there is major business process change.

Check Your Progress 4

1) Action oriented plan would be easy for reference at speed.

2) The outcomes of the plan include a documented plan for each department or business unit, criteria for BU to escalate issue to BCT and clearly defined BCM roles within the department.

3) The plan should be reviewed when there is a major change in the business process or technology within that area.

3.9 SUGGESTED READINGS

- "A G ، Continuity Planning" by James C. Barnes
- BS 25999-1:2006 Business Continuity Management Part 1: Code of practice
- BS 25999-2:2007 Business Continuity Management Part 2: Specification
- "Business Continuity Planning", A Step-by-Step Guide with Planning Forms on CDROM by Kenneth L Fulmer
- "Disaster Survival Planning: A Practical Guide for Businesses" by Judy Bell
- en.wikipedia.org/wiki/Business continuity planning

UNIT 4 DISASTER SIMULATION EXERCISE

Structure

4.0 INTRODUCTION

In this unit we have to study about the Disaster and Disaster Simulation exercise. WHO defines Disaster as "any occurrence that causes damage, ecological disruption, loss of human life, deterioration of health and health services, on a scale sufficient to warrant an extraordinary response from outside the affected community or area."

Disasters can be defined in different ways.

- A disaster is an overwhelming ecological disruption occurring on a scale sufficient to require outside assistance
- A disaster is an event located in time and space which produces conditions whereby the continuity of structure and process of social units becomes problematic
- It is an event or series of events which seriously disrupts normal activities

Simulation is the imitation of some real thing, state of affairs, or process. The act of simulating something generally entails representing certain key characteristics or behaviors of a selected physical or abstract system.

Simulation is used in many contexts, such as simulation of technology for performance optimization, safety engineering, testing, training, disaster management , education, and video games. Training simulators include flight simulators for training aircraft pilots in order to provide them with a lifelike experience. Simulation is also used for scientific modeling of natural systems or human systems in order to gain insight into their functioning. Simulation can be used to show the eventual real effects of alternative conditions and courses of action. Simulation is also used when the real system cannot be engaged, because it may not be accessible, or it may be dangerous or unacceptable to engage, or it is being designed but not yet built, or it may simply not exist.

Key issues in simulation include acquisition of valid source information about the relevant selection of key characteristics and behaviors, the use of simplifying approximations and assumptions within the simulation, and fidelity and validity of the simulation outcomes.

4.1 OBJECTIVES

After studying this unit, you should be able to:

- understand about Disaster and Disaster Simulation;
- types of Disaster , Risks of hazards, vulnerability, hazards;
- disaster management program;
- safety tips for Different Disaster as a part of DMP;
- some fundamental aspects of DMP; and
- disaster simulation Exercise.

4.2 WHAT IS DISASTER?

Disaster is a sudden, calamitous event bringing great damage, loss, and destruction and devastation to life and property. The damage caused by disasters is immeasurable and varies with the geographical location, climate and the type of the earth surface/degree of vulnerability. This influences the mental, socio-economic, political and cultural state of the affected area. Generally, disaster has the following effects in the concerned areas,

1. It completely disrupts the normal day to day life
2. It negatively influences the emergency systems
3. Normal needs and processes like food, shelter, health, etc. are affected and deteriorate depending on the intensity and severity of the disaster.

It may also be termed as "a serious disruption of the functioning of society, causing widespread human, material or environmental losses which exceed the ability of the affected society to cope using its own resources."

Thus, a disaster may have the following main features:-

- Unpredictability
- Unfamiliarity
- Speed
- Urgency
- Uncertainty
- Threat

Thus, in simple terms we can define disaster as a hazard causing heavy loss to life, property and livelihood. E.g. a cyclone killing 10,000 lives and a crop loss of one crore can be termed as disaster.

4.3 TYPES OF DISASTERS

Generally, disasters are of two types – **Natural** and **Manmade**. Based on the devastation, these are further classified into major/minor natural disaster and major/minor manmade disasters. Some of the disasters are listed below,

Major natural disasters:	**Minor natural disasters:**
• Flood • Cyclone • Drought • Earthquake	• Cold wave • Thunderstorms • Heat waves • Mud slides • Storm

Major manmade disaster:	Minor manmade disaster:
• Setting of fires • Epidemic • Deforestation • Pollution due to prawn cultivation • Chemical pollution. • Wars	• Road / train accidents, riots • Food poisoning • Industrial disaster/ crisis • Environmental pollution

Risk

Risk is a measure of the expected losses due to a hazardous event of a particular magnitude occurring in a given area over a specific time period. Risk is a function of the probability of particular occurrences and the losses each would cause. The level of risk depends on:

- Nature of the Hazard
- Vulnerability of the elements which are affected
- Economic value of those elements

Vulnerability

It is defined as *"the extent to which a community, structure, service, and/or geographic area is likely to be damaged or disrupted by the impact of particular hazard, on account of their nature, construction and proximity to hazardous terrain or a disaster prone area"*

Hazards

Hazards are defined as *"Phenomena that pose a threat to people, structures, or economic assets and which may cause a disaster. They could be either manmade or naturally occurring in our environment."*

4.4 DISASTER MANAGEMENT PROGRAM (DMP)

The extent of damage in a disaster depends on:

1) The impact, intensity and characteristics of the phenomenon and
2) How people, environment and infrastructures are affected by that phenomenon

This relationship can be written as an equation:

Government of India [GoI], Ministry of Home Affairs [MHA] and United Nations Development Programme [UNDP] have signed an agreement on

August 2002 for implementation of ***"Disaster Risk Management"*** Programme to reduce the vulnerability of the communities to natural disasters, in identified multi–hazard disaster prone areas.

Goal: "Sustainable Reduction in Natural Disaster Risk" in some of the most hazard prone districts in selected states of India".

The four main ***objectives*** of this programme are:

1. National capacity building support to the Ministry of Home Affairs
2. Environment building, education, awareness programme and strengthening the capacity at all levels in natural disaster risk management and sustainable recovery
3. Multi-hazard preparedness, response and mitigation plans for the programme at state, district, block and village/ward levels in select programme states and districts
4. Networking knowledge on effective approaches, methods and tools for natural disaster risk management, developing and promoting policy frameworks

Programme Phases

The programme has been divided into two phases over a period of six years. Phase I [2002-2004] would provide support to carry out the activities in 28 select districts in the states of Bihar, Gujarat and Orissa. In phase II [2003-2007], the Programme would cover 141 districts in the states of Assam, Meghalaya, Sikkim, West Bengal, Uttaranchal, Uttar Pradesh, Delhi, Maharashtra, Tamilnadu, Manipur, Mizoram, Tripura, Arunachal Pradesh and Nagaland.

Special Focus: 38 Earthquake prone cities having more than half a million population

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 disaster?

.....

.....

.....

.....

2) How may be disaster classified?

.....

.....

.....

.....

3) What is Disaster Management Program and what its goal?

.....

.....

.....

.....

4.5 SAFETY TIPS FOR DIFFERENT DISASTER AS A PART OF DMP

Earthquakes – usually give no warning at all.

Safety Tips

Prepare your family - Before the earthquake

Now is the time to formulate a safety plan for you and your family. If you wait until the earth starts to shake, it may be too late. Consider the following safety measures:

- Always keep the following in a designated place: bottled drinking water, non-perishable food (chura, gur, etc), first-aid kit, torchlight and battery-operated radio with extra batteries.
- Teach family members how to turn off electricity, gas, etc.
- Identify places in the house that can provide cover during an earthquake.
- It may be easier to make long distance calls during an earthquake. Identify an out-of-town relative or friend as your family's emergency contact. If the family members get separated after the earthquake and are not able to contact each other, they should contact the designated relative/friend. The address and phone number of the contact person/relative should be with all the family members.

Safeguard your house

- Consider retrofitting your house with earthquake-safety measures. Reinforcing the foundation and frame could make your house quake

resistant. You may consult a reputable contractor and follow building codes.

- Kutchha buildings can also be retrofitted and strengthened.

During quake

Earthquakes give no warning at all. Sometimes, a loud rumbling sound might signal its arrival a few seconds ahead of time. Those few seconds could give you a chance to move to a safer location. Here are some tips for keeping safe during a quake.

- Take cover. Go under a table or other sturdy furniture; kneel, sit, or stay close to the floor. Hold on to furniture legs for balance. Be prepared to move if your cover moves.
- If no sturdy cover is nearby, kneel or sit close to the floor next to a structurally sound interior wall. Place your hands on the floor for balance.
- Do not stand in doorways. Violent motion could cause doors to slam and cause serious injuries. You may also be hit be flying objects.
- Move away from windows, mirrors, bookcases and other unsecured heavy objects.
- If you are in bed, stay there and cover yourself with pillows and blankets
- Do not run outside if you are inside. Never use the lift.
- If you are living in a kutccha house, the best thing to do is to move to an open area where there are no trees, electric or telephone wires.

If outdoors

- Move into the open, away from buildings, streetlights, and utility wires. Once in the open, stay there until the shaking stops.
- If your home is badly damaged, you will have to leave. Collect water, food, medicine, other essential items and important documents before leaving.
- Avoid places where there are loose electrical wires and do not touch metal objects that are in touch with the loose wires.
- Do not re-enter damaged buildings and stay away from badly damaged structures.

If in a moving vehicle

Move to a clear area away from buildings, trees, overpasses, or utility wires, stop, and stay in the vehicle. Once the shaking has stopped, proceed with caution. Avoid bridges or ramps that might have been damaged by the quake.

After the quake

Here are a few things to keep in mind after an earthquake. The caution you display in the aftermath can be essential for your personal safety.

- Wear shoes/chappals to protect your feet from debris
- After the first tremor, be prepared for aftershocks. Though less intense, aftershocks cause additional damages and may bring down weakened structures. Aftershocks can occur in the first hours, days, weeks, or even months after the quake.
- Check for fire hazards and use torchlights instead of candles or lanterns.
- If the building you live in is in a good shape after the earthquake, stay inside and listen for radio advises. If you are not certain about the damage to your building, evacuate carefully. Do not touch downed power line.
- Help injured or trapped persons. Give first aid where appropriate. Do not move seriously injured persons unless they are in immediate danger of further injury. In such cases, call for help.
- Remember to help your neighbours who may require special assistance-infants, the elderly, and people with disabilities.
- Listen to a battery-operated radio for the latest emergency information.
- Stay out of damaged buildings.
- Return home only when authorities say it is safe. Clean up spilled medicines, bleaches or gasoline or other flammable liquids immediately. Leave the area if you smell gas or fumes from other chemicals. Open closet and cupboard doors cautiously.
- If you smell gas or hear hissing noise, open windows and quickly leave the building. Turn off the switch on the top of the gas cylinder.
- Look for electrical system damages - if you see sparks, broken wires, or if you smell burning of amber, turn off electricity at the main fuse box. If you have to step in water to get to the fuse box, call an electrician first for advice.

- Check for sewage and water lines damage. If you suspect sewage lines are damaged, avoid using the toilets. If water pipes are damaged, avoid using water from the tap.
- Use the telephone only for emergency calls.
- In case family members are separated from one another during an earthquake (a real possibility during the day when adults are at work and children are at school), develop a plan for reuniting after the disaster. Ask an out of state / district relative or friend to serve as the "family contact". Make sure everyone in the family knows the name, address, and phone number(s) of the contact person (s).

Cyclone

Safety Tips

Before the Cyclone Season

Keep watch on weather and listen to radio or TV. Keep alert about the community warning systems – loudspeakers, bells, conches, drums or any traditional warning system.

- Get to know the nearest cyclone shelter / safe houses and the safest route to reach these shelters.
- Do not listen to rumours.
- Prepare an emergency kit containing:
- A portable radio, torch and spare batteries;
- Stocks dry food: Chura, Chhatua, Mudhi, gur etc.
- Matches, fuel lamp, portable stove, cooking utensils, waterproof bags
- A first aid kit, manual etc.
- Katuri, pliers, small saw, axe and plastic rope

Check the roof and cover it with net or bamboo. Check the walls, pillars, doors and windows to see if they are secure. If not, repair those at the earliest. In case of tin roofs, check the condition of the tin and repair the loose points. Cover the mud walls with polythene or coconut leaves mats or straw mats on a bamboo frame. Bind each corner of the roof with a plastic rope in case of thatched roof.

- Trim dry tree branches, cut off the dead trees and clear the place/courtyard of all debris, including coconuts and tree branches.
- Clear your property of loose materials that could blow about and cause injury or damage during extreme winds.

- If your area is prone to storm surge, locate safe high ground or shelter.
- Keep important documents, passbook, etc. in a tight plastic bag and take it along with your emergency kits if you are evacuating.
- Identify the spot where you can dig holes to store food grains, seeds, etc. in polythene bags.
- Keep a list of emergency addresses and phone numbers on display. Know the contact telephone number of the government offices /agencies, which are responsible for search, rescue and relief operations in your area.

If you are living in an area where CBDP exercises have taken place, ensure:

- Vulnerability list and maps have been updated
- Cyclone drill including search and rescue, first aid training have taken place
- Stock of dry food, essential medicines and proper shelter materials maintained

Upon a cyclone warning

- Store loose items inside. Put extra agricultural products/ stock like paddy in plastic bags and store it by digging up a hole in the ground, preferably at a higher elevation and then cover it properly. Fill bins and plastic jars with drinking water.
- Keep clothing for protection, handy
- Prepare a list of assets and belongings of your house and give information to volunteers and other authorities about your near and dear ones.
- Fill fuel in your car/motorcycle and park it under a solid cover. Tie bullock carts, boats securely to strong posts in an area, which has a strong cover and away from trees. Fallen trees can smash boats and other assets.
- Close shutters or nail all windows. Secure doors. Stay indoors, with pets.
- Pack warm clothing, essential medications, valuables, papers, water, dry food and other valuables in waterproof bags, to be taken along with your emergency kit.
- Listen to your local radio / TV, local community warning system for further information.

- In case of warning of serious storm, move with your family to a strong pucca building. In case of warning of cyclones of severe intensity, evacuate the area with your family, precious items and documents and emergency kit. Take special care for children, elders, sick, pregnant women and lactating mothers in your family. Do not forget your emergency food stock, water and other emergency items. **Go To The Nearest Cyclone Shelter.**
- Do not venture into the sea for fishing.

On warning of local evacuation

Based on predicted wind speeds and storm surge heights, evacuation may be necessary. Official advice may be given on local radio / TV or other means of communication regarding safe routes and when to move.

- Wear strong shoes or chappals and clothing for protection.
- Lock your home, switch off power, gas, water, and take your emergency kit.
- If evacuating to a distant place take valuable belonging, domestic animals, and leave early to avoid heavy traffic, flooding and wind hazards.
- If evacuating to a local shelter or higher grounds carry the emergency kit and minimum essential materials.

When the cyclone strikes

- Disconnect all electrical appliances and turn off gas.
- If the building starts crumbling, protect yourself with mattresses, rugs or blankets under a strong table or bench or hold on to a solid fixture (e.g. a water pipe)
- Listen to your transistor radio for updates and advice.
- Beware of the calm `eye'. If the wind suddenly drops, don't assume the cyclone is over; violent winds will soon resume from the opposite direction. Wait for the official **"all clear"**.
- If driving, stop – but well away from the sea and clear of trees, power lines and watercourses. Stay in the vehicle.

After the cyclone

- Do not go outside until officially advised it is safe.
- Check for gas leaks. Do not use electric appliances, if wet.

- Listen to local radio for official warnings and advice.
- If you have to evacuate, or did so earlier, do not return until advised. Use a recommended route for returning and do not rush.
- Be careful of snake bites and carry a stick or bamboo
- Beware of fallen power lines, damaged bridges, buildings and trees, and do not enter the floodwaters.
- Heed all warnings and do not go sightseeing.

Floods

Safety Tips

This guide lists simple things you and your family can do to stay safe and protect your property from floods.

Before Flooding Occurs

- All your family members should know the safe route to nearest shelter/ raised pucca house.
- If your area is flood-prone, consider alternative building materials. Mud walls are more likely to be damaged during floods. You may consider making houses where the walls are made of local bricks up to the highest known flood level with cement pointing.
- Have an emergency kit on hand which includes a:
    - A portable radio, torch and spare batteries;
    - Stocks of fresh water, dry food (chura, mudi, gur, biscuits), kerosene, candle and matchboxes;
    - Waterproof or polythene bags for clothing and valuables, an umbrella and bamboo stick (to protect from snake), salt and sugar.
    - A first aid kit, manual and strong ropes for tying things

When you hear a flood warning or if flooding appears likely

- Tune to your local radio/TV for warnings and advice.
    - Keep vigil on flood warning given by local authorities
    - Don't give any importance to rumours and don't panic
    - Keep dry food, drinking water and clothes ready

- Prepare to take bullock carts, other agricultural equipments, and domestic animals to safer places or to higher locations.
- Plan which indoor items you will raise or empty if water threatens to enter your house
- Check your emergency kit

During floods

- Drink boiled water.
- Keep your food covered, don't take heavy meals.
- Use raw tea, rice-water, tender coconut-water, etc. during diarrhea; contact your ANM/AWW for ORS and treatment.
- Do not let children remain on empty stomach.
- Use bleaching powder and lime to disinfect the surrounding.
- Help the officials/volunteers distributing relief materials.

If you need to evacuate

- Firstly pack warm clothing, essential medication, valuables, personal papers, etc. in waterproof bags, to be taken with your emergency kit.
- Take the emergency kit
- Inform the local volunteers (if available), the address of the place you are evacuating to.
- Raise furniture, clothing and valuables onto beds, tables and to the top of the roof (electrical items highest).
- Turn off power.
- Whether you leave or stay, put sandbags in the toilet bowl and over all laundry / bathroom drain-holes to prevent sewage back-flow.
- Lock your home and take recommended/known evacuation routes for your area.
- Do not get into water of unknown depth and current.

If you stay or on your return

- Stay tuned to local radio for updated advice.
- Do not allow children to play in, or near, flood waters.

- Avoid entering floodwaters. If you must, wear proper protection for your feet and check depth and current with a stick. Stay away from drains, culverts and water over knee-deep.
- Do not use electrical appliances, which have been in floodwater until checked for safety.
- Do not eat food, which has been in floodwaters.
- Boil tap water (in cities) until supplies have been declared safe. In case of rural areas, store tube well water in plastic jars or use halogen tablets before drinking.
- Be careful of snakes, snakebites are common during floods.

Flooding and Storm Surges along the Coastline

Tsunamis

Tsunamis are Ocean Waves produced by Earth Quakes or Underwater land slides. The word is Japanese and means "Harbor Waves" Tsunami is actually a series of waves that can travel at speeds from 400-600 mph in the open ocean. As the waves approach the coast, their speed decreases, but their amplitude increases. Unusual wave heights of 10-20 ft high can be very destructive and cause many deaths and injuries. Most deaths caused by Tsunamis are because of Drowning.

Associated risks include Flooding, Contamination of Drinking Water, Fires from ruptured gas lines and tanks, Loss of vital Community Infrastructure [police, fire, medical], Areas of greatest risks are - Less than 25 feet above sea level, Within 1 mile of the shore line.

Environmental Conditions left by the Tsunamis may contribute to the transmission of the following diseases

From Food or Water

- Diarrhea illnesses; Cholera, Acute Diarrhea, Dysentery
- Hepatitis-A, Hepatitis-E
- Typhoid Fever
- Food borne illnesses; Bacterial; Viral; Parasitic; Non-infections;

From Animals or Mosquitoes

- Leptospirosis, Plague, Malaria, J.E, Dengue, Rabies
- Respiratory Diseases; Avian flu, Influenza, Measles

Effects of Nuclear Holocaust: The effects of nuclear holocaust will result into blasts, heat storms, secondary fires, fire, ionizing radiation and fall outs.

These effects fall into 3 categories;

1) Immediate, 2) Short term and 3) Long term effects.

- **The immediate effects:** This includes blast effects, heat effects, electromagnetic pulse (EMP) effects and radiation effects.
- **The short term effects:** This include problems connected with water supply, sanitation, food, dispersal of excreta, wastes and dead bodies, break down of vector control measures and outbreak of infections. Radioactive contamination of water and food are major concerns. The affected area creates a lot of other problems for the survivors and the rescue teams. Major problem among survivors is of bone marrow depression resulting in leucopenia, which increases their susceptibility to infections
- **Long term effects:** The knowledge about the long-term effects is still incomplete. Some well known effects include radiation injuries due to radiation fallout, suppression of body immunity, chronic infection and other associated illnesses.

Persistent radiation hazards will lead to prolonged contamination of water supply, increased ultraviolet radiation, climatic and ecological disturbances, psychological disturbances and genetic abnormalities.

Tips on Fire Accidents

a) High-Rise Fires

- Calmly leave the apartment, closing the door behind you. Remember the keys!
- Pull the fire alarm near the closest exit, if available, or raise an alarm by warning others.
- Leave the building by the stairs.
- Never take the elevator during fire!

If the exit is blocked by smoke or fire

- Leave the door closed but do not lock it.
- To keep the smoke out, put a wet towel in the space at the bottom of the door.

- Call the emergency fire service number and tell them your apartment number and let them know you are trapped by smoke and fire. It is important that you listen and do what they tell you.
- Stay calm and wait for someone to rescue you.

If there is a fire alarm in your building which goes off

- Before you open the door, feel the door by using the back of our hand. If the door is hot or warm, do not open the door.
- If the door is cool, open it just a little to check the hallway. If you see smoke in the hallway, do not leave.
- If there is no smoke in the hallway, leave and close the door. Go directly to the stairs to leave. Never use the elevator.

If smoke is in your apartment

- Stay low to the floor under the smoke.
- Call the Fire Emergency Number which should be pasted near your telephone along with police and other emergency services and let them know that you are trapped by smoke.
- If you have a balcony and there is no fire below it, go out.
- If there is fire below, go out to the window. **Do Not Open the Window** but stay near the window.
- If there is no fire below, go to the window and open it. Stay near the open window.
- Hang a bed sheet, towel or blanket out of the window to let people know that you are there and need help.
- Be calm and wait for someone to rescue you.

b) Kitchen Fires

It is important to know what kind of stove or cooking oven you have in your home – gas, electric, kerosene or where firewood is used. The stove is the No. 1 cause of fire hazards in your kitchen and can cause fires, which may destroy the entire house, especially in rural areas where there are thatched roof or other inflammable materials like straw kept near the kitchen. For electric and gas stoves **ensure that the switch or the gas valve is switched off/turned off immediately after the cooking is over.** An electric burner remains hot and **until it cools off, it can be very dangerous**. The oven using wood can be dangerous because burning embers remain. When lighting the fire on a wooden fuel oven, **keep a cover on the top** while lighting the oven so that sparks do

not fly to the thatched roof. After the cooking is over, ensure that the remaining **fire is extinguished off by sprinkling water** if no adult remains in the kitchen after the cooking. **Do not keep any inflammable article like kerosene near the kitchen fire.**

Important Do's in the Kitchen

- **Do** have an adult always present when cooking is going on the kitchen. Children should not be allowed alone.
- **Do** keep hair tied back and do not wear synthetic clothes when you are cooking.
- **Do** make sure that the curtains on the window near the stove are tied back and will not blow on to the flame or burner.
- **Do** check to make sure that the gas burner is turned off immediately if the fire is not ignited and also switched off immediately after cooking.
- **Do** turn panhandles to the centre of the stove and put them out of touch of the children in the house.
- **Do** ensure that the floor is always dry so that you do not slip and fall on the fire.
- **Do** keep matches out of the reach of children.

Important Don'ts

- **Don't** put towels, or dishrags near a stove burner.
- **Don't** wear loose fitting clothes when you cook, and **don't** reach across the top of the stove when you are cooking.
- **Don't** put things in the cabinets or shelves above the stove. Young children may try to reach them and accidentally start the burners, start a fire, catch on fire.
- **Doesn't store** spray cans or cans carrying inflammable items near the stove.
- **Don't** let small children near an open oven door. They can be burnt by the heat or by falling onto the door or into the oven.
- **Don't** lean against the stove to keep warm.
- **Don't** use towels as potholders. They may catch on fire.
- **Don't** overload an electrical outlet with several appliances or extension cords. The cords or plugs may overheat and cause a fire.

- **Don't** use water to put out a grease fire. ONLY use baking soda, salt, or a tight lid. Always keep a box of baking soda near the stove.
- **Don't** use radios or other small appliances (mixers, blenders) near the sink.

Common Tips

- **Do** keep the phone number of the Fire Service near the telephone and ensure that everyone in the family knows the number.
- **Do** keep matches and lighters away from children.
- **Do** sleep with your bedroom closed to prevent the spread of fire.

Do you know that you should **never run** if your **clothes are on fire** and that you **should - "Stop – Drop-Roll."**

Landslide

During a Landslide

- Stay alert and awake. Many debris-flow fatalities occur when people are sleeping. Listen to a Weather Radio or portable, battery-powered radio or television for warnings of intense rainfall. Be aware that intense, short bursts of rain may be particularly dangerous, especially after longer periods of heavy rainfall and damp weather.
- If you are in areas susceptible to landslides and debris flows, consider leaving if it is safe to do so. Remember that driving during an intense storm can be hazardous. If you remain at home, move to a second story if possible. Staying out of the path of a landslide or debris flow saves lives.
- Listen for any unusual sounds that might indicate moving debris, such as trees cracking or boulders knocking together. A trickle of flowing or falling mud or debris may precede larger landslides. Moving debris can flow quickly and sometimes without warning.
- If you are near a stream or channel, be alert for any sudden increase or decrease in water flow and for a change from clear to muddy water. Such changes may indicate landslide activity upstream, so be prepared to move quickly. Don't delay! Save yourself, not your belongings.
- Be especially alert when driving. Embankments along roadsides are particularly susceptible to landslides. Watch the road for collapsed pavement, mud, fallen rocks, and other indications of possible debris flows.

What to Do if You Suspect Imminent Landslide Danger:

- Contact your local fire, police, or public works department. Local officials are the best persons able to assess potential danger.
- Inform affected neighbors. Your neighbors may not be aware of potential hazards. Advising them of a potential threat may help save lives. Help neighbors who may need assistance to evacuate.
- Evacuate. Getting out of the path of a landslide or debris flow is your best protection.

Media and Community Education Ideas

- In an area prone to landslides, publish a special newspaper section with emergency information on landslides and debris flows. Localize the information by including the phone numbers of local emergency services offices, the Red Cross, and hospitals.
- Report on what city and county governments are doing to reduce the possibility of landslides. Interview local officials about local land- use zoning regulations.
- Interview local officials and major insurers. Find out if debris flow is covered by flood insurance policies and contact your local emergency management office to learn more about the program.
- Work with local emergency services to prepare special reports for people with mobility impairments on what to do if evacuation is ordered.
- Support your local government in efforts to develop and enforce land-use and building ordinances that regulate construction in areas susceptible to landslides and debris flows. Buildings should be located away from steep slopes, streams and rivers, intermittent-stream channels, and the mouths of mountain channels.

After the Landslide

- Stay away from the slide area. There may be danger of additional slides.
- Check for injured and trapped persons near the slide, without entering the direct slide area. Direct rescuers to their locations.
- Help a neighbor who may require special assistance - infants, elderly people, and people with disabilities. Elderly people and people with disabilities may require additional assistance. People who care for them or who have large families may need additional assistance in emergency situations.

- Listen to local radio or television stations for the latest emergency information.
- Watch for flooding, which may occur after a landslide or debris flow. Floods sometimes follow landslides and debris flows because they may both be started by the same event.
- Look for and report broken utility lines to appropriate authorities. Reporting potential hazards will get the utilities turned off as quickly as possible, preventing further hazard and injury.
- Check the building foundation, chimney, and surrounding land for damage. Damage to foundations, chimneys, or surrounding land may help you assess the safety of the area.
- Replant damaged ground as soon as possible since erosion caused by loss of ground cover can lead to flash flooding.
- Seek the advice of a geotechnical expert for evaluating landslide hazards or designing corrective techniques to reduce landslide risk. A professional will be able to advise you of the best ways to prevent or reduce landslide risk, without creating further hazard.

Media and Community Education Ideas

- In an area prone to landslides, publish a special newspaper section with emergency information on landslides and debris flows. Localize the information by including the phone numbers of local emergency services offices, the American Red Cross chapter, and hospitals.
- Report on what city and county governments are doing to reduce the possibility of landslides. Interview local officials about local land- use zoning regulations.
- Interview local officials and major insurers regarding the National Flood Insurance Program. Find out if debris flow is covered by flood insurance policies from the National Flood Insurance Program and contact your local emergency management office to learn more about the program.
- Work with local emergency to prepare special reports for people with mobility impairments on what to do if evacuation is ordered.
- Support your local government in efforts to develop and enforce land-use and building ordinances that regulate construction in areas susceptible to landslides and debris flows. Buildings should be located away from steep slopes, streams and rivers, intermittent-stream channels, and the mouths of mountain channels.

Before a Landslide: How to Plan

Develop a Family Disaster Plan. Please see the "Family Disaster Plan" section for general family planning information. Develop landslide-specific planning.

Learn about landslide risk in your area. Contact local officials, state geological surveys or departments of natural resources, and university departments of geology. Landslides occur where they have before, and in identifiable hazard locations. Ask for information on landslides in your area, specific information on areas vulnerable to landslides, and request a professional referral for a very detailed site analysis of your property, and corrective measures you can take, if necessary.

If you are at risk from landslides

- Talk to your insurance agent.
- Develop an evacuation plan.
- Discuss landslides and debris flow with your family. Everyone should know what to do in case all family members are not together. Discussing disaster ahead of time helps reduce fear and lets everyone know how to respond during a lands.

4.6 FUNDAMENTAL ASPECTS OF DMP

Six Fundamental Aspects of Disaster Management

There are 6 fundamental aspects of Disaster Management like

1) Disaster prevention
2) Disaster Preparedness
3) Disaster Response
4) Disaster Mitigation
5) Rehabilitation
6) Reconstruction

These 6 aspects of Disaster Management corresponds to the 2 phases in the Disaster Cycle, i.e.

1. Risk Reduction Phase, before a Disaster
2. Recovery Phase, after Disaster problems as they arise.

4.6.1 Disaster Prevention

Existing knowledge that might reduce the undesirable effects of disasters is often not applied.

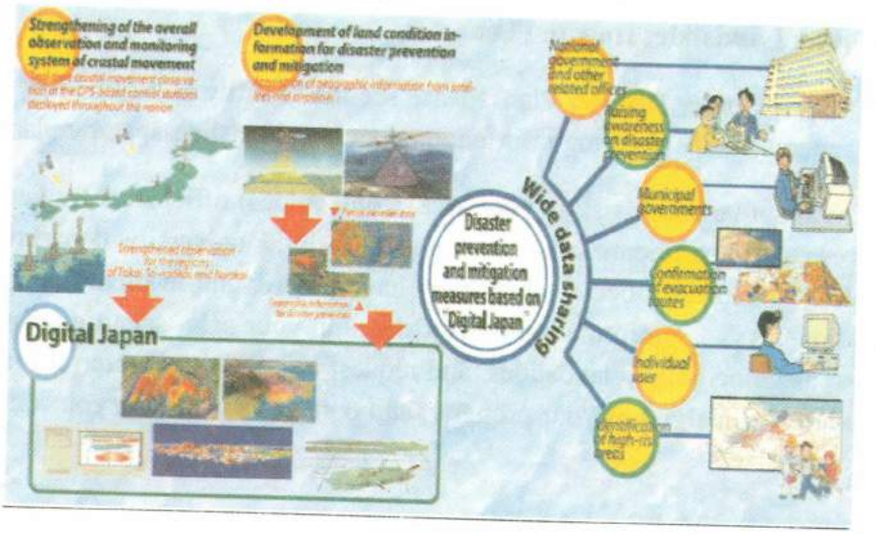

Fig.1

- Hurricane/Tornado/ Cyclone warning systems
- Legislation preventing building in the flood prone areas
- Requirement of protective cellars/shelters in disaster prone areas
- A Seismic housing code for earthquake-prone area
- Strict procedural code followed to prevent Nuclear, Toxicological and Chemical disasters

Early warning systems and Disaster preparedness which will help to minimize morbidity, mortality and economic loss

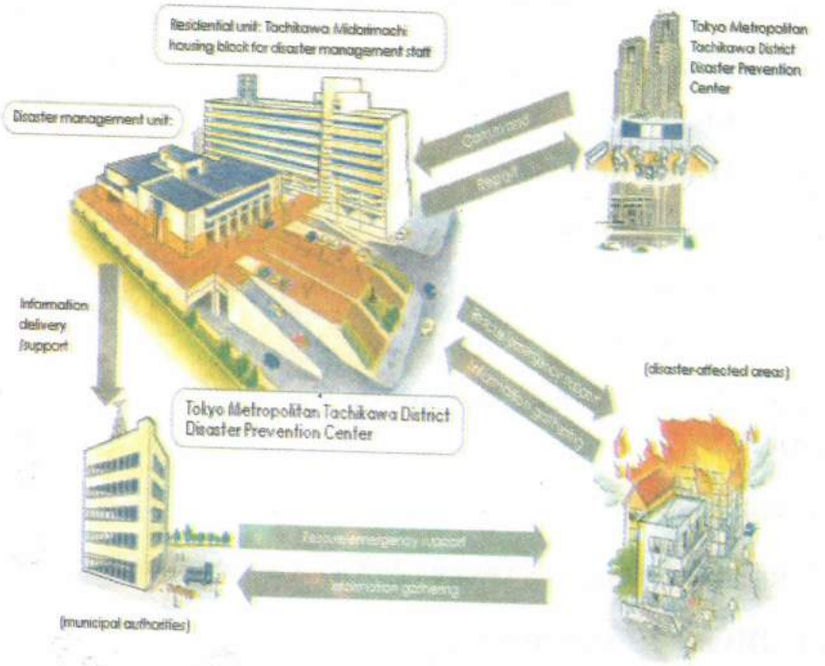

Fig.2

Family Disaster Plan

- Discuss the type of hazards that could affect your family. Know your home's vulnerability to storm surge, flooding and wind.
- Locate a safe room or the safest areas in your home for each hurricane hazard. In certain circumstances the safest areas may not be your home but within your community.
- Determine escape routes from your home and places to meet.
- Have an out-of-state friend as a family contact, so all your family members have a single point of contact.
- Make a plan now for what to do with your pets if you need to evacuate.
- Post emergency telephone numbers by your phones and make sure your children know how and when to call 911.
- Check your insurance coverage - flood damage is not usually covered by homeowners insurance. National Flood Insurance Program
- Stock non-perishable emergency supplies and a Disaster Supply Kit.
- Use a NOAA weather radio. Remember to replace its battery every 6 months, as you do with your smoke detectors.
- Take First Aid, CPR and disaster preparedness classes.

4.6.2 Disaster Preparedness

The objectives of the disaster preparedness is to ensure that appropriate systems, procedures and resources are in place to provide prompt, effective assistance to disaster victims, thus facilitating relief measures and rehabilitation services.

Disaster preparedness is an ongoing, multi-sectoral activity to carry out the following activities:

- Evaluate the risk of the country or particular region to disasters.
- Adopt standards and regulations
- Organize communication, information and warning systems
- Ensure coordination and response mechanisms
- Adopt measures to ensure that financial and other resources are available for increased readiness and can be mobilized in disaster situations.
- Develop public education programs
- Coordinate information sessions with news media

- Organize disaster simulation exercises that test response mechanisms

For the Health Sectors Disaster Preparedness plan to be successful, clear mechanisms for coordinating with other sectors and internationally must be in place.

The Health Disaster Coordinator is in charge of preparedness activities and coordinating plans with

- Govt. Agencies
- Foreign Relations- UN,UNICEF.WHO and other international agencies
- NGO's- Red Cross etc
- Those responsible for power, communication, Housing, water services etc
- Civil Protection agencies-Police, armed forces

Emergency Preparedness

Agents, Diseases and Other Threats

1. Natural Disasters – like Earthquakes, Floods, Cyclones, Typhoons, Tsunamis, winter
2. Bio-Terrorism Agents – like Anthrax, Plague, Smallpox
3. Chemical Emergencies - Ricin, Phosgene, Bromine, Sarin
4. Radioactive Emergencies
5. Mass Trauma - Explosions, Blasts, Burns, Injuries
6. Recent Outbreaks and Incidents - Bird flu, SARS, West Nile Virus, Mad Cow Disease

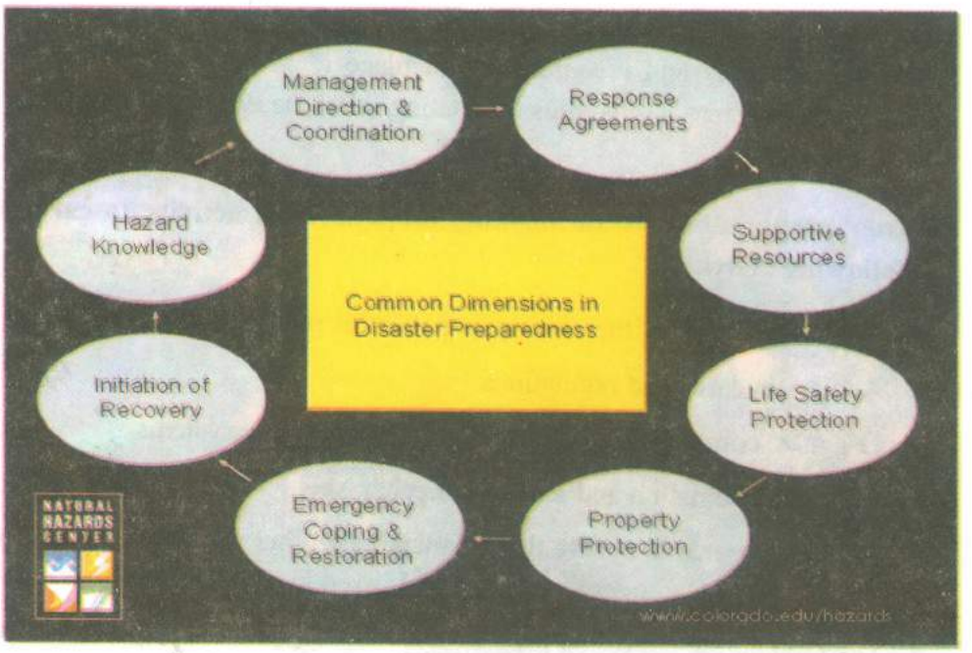

Fig.3

4.6.3 Disaster Response

Objectives

- Appropriate application of current technology can prevent much of the death, injury, and economic disruption resulting from disasters
- Morbidity and mortality resulting from disasters differ according to the type and location of the event.
- In any disaster, prevention should be directed towards reducing

  (1) Losses due to the disaster event itself

  (2) Losses resulting from the Mismanagement of disaster relief.

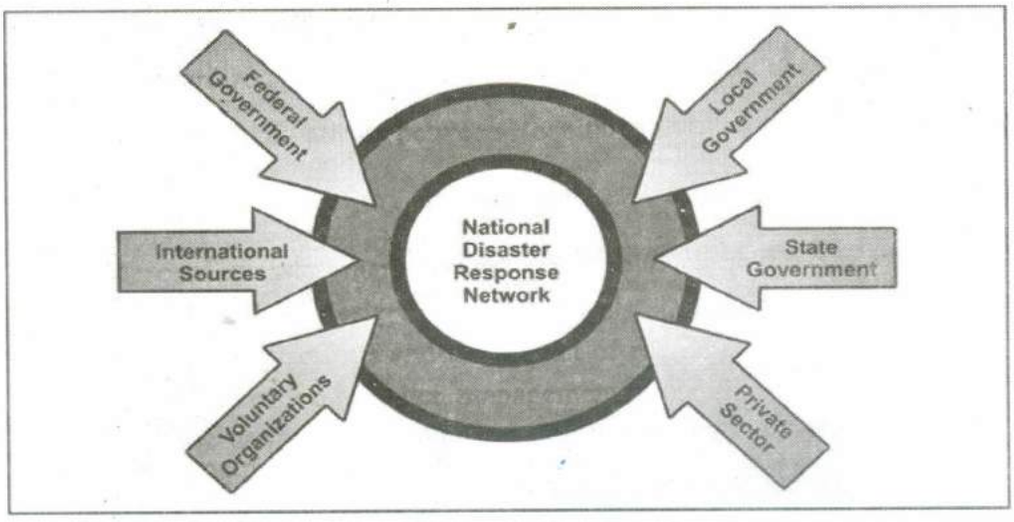

Fig.4

Therefore, the public health objectives of disaster management can be stated as follows:

1. Prevent unnecessary morbidity, mortality and economic loss resulting directly from the disaster.
2. Eliminate morbidity, mortality and economic loss directly attributable to Mismanagement of disaster relief efforts.

Nature and Extent of the Problem

Morbidity and mortality, which result from a disaster situation, can be classified into four types:

1. Injuries,
2. Emotional stress,
3. Epidemics of diseases,
4. Increase in indigenous diseases.

The relative numbers of deaths and injuries differ on the type of disaster.

Injuries usually exceed deaths in explosions, typhoons, hurricanes, fires, famines, tornadoes, and epidemics.

Deaths frequently exceed injuries in landslides, avalanches, volcanic eruptions, tidal waves, floods, and earthquakes.

Disaster victims often exhibit emotional stress or the **"disaster shock" syndrome**. The syndrome consists of successive stages of shock, suggestibility, euphoria and frustration.

Each of these stages may vary in extent and duration depending on other factors.

Epidemics are included in the definition of disaster; however, they can also be the result of other disaster situations.

Diseases, which may be associated with disasters, include

- specific food and/or water bone illnesses

  (e.g., typhoid, gastroenteritis and cholera),
- vector bone illnesses

  (e.g., plague and malaria),
- diseases spread by person-to-person contact

  (e.g., hepatitis A and shigellosis)
- Diseases spread by the respiratory route

  (e.g., measles and influenza).
- The current status of environmental sanitation, disease surveillance, and preventive medicine has led to a significant reduction in the threat of epidemics following disaster.
- Immunization programs are rarely indicated as a specific post disaster measure.
- A disaster is often followed by an increase in the prevalence of diseases indigenous to the area due to the disruption of medical and other health facilities and programs.

Morbidity and Mortality from Mismanagement of Relief

Ideally, attempts to mitigate the results of a disaster would not add to the negative consequences;

However, there have been many instances in which inappropriate and/or incomplete management actions taken after a disaster contributed to unnecessary morbidity, mortality, and a waste of resources.

Many of the Causalities and much more of the Destruction occurring to natural disaster are due to ignorance and neglect on the part of the individuals and public authorities.

There is a plethora of literature describing the inappropriate actions taken to manage past disasters. Many of the same mismanagement problems tend to recur.

- Physicians and nurses have been sent into disaster areas in numbers far in excess of actual need.
- Medical and paramedical personnel have often been hampered by the lack of the specific supplies they need to apply their skills to the disaster situation.
- In some disasters, available supplies have not been inventoried until well after the disaster, resulting in the importation of material which is used or needed.

In a study of past disaster mismanagement problems and their causes, these problems were categorized as follows:

1. Inadequate appraisal of damages
2. Inadequate problem ranking
3. Inadequate identification of resources
4. Inadequate location of resources
5. Inadequate transportation of resources
6. Inadequate utilization of resources

4.6.4 Disaster Mitigation

It is virtually impossible to prevent occurrence of most Natural Disasters, but it is possible to minimize or mitigate their damage effects.

Mitigation measures aim to reduce the Vulnerability of the System [eg. By improving and enforcing building codes etc]

Disaster prevention implies complete elimination of damages from a hazard, but it is not realistic in most hazards. [eg. Relocating a population from a flood plain or from beach front]

Medical Casualty could be drastically reduced by improving the Structural Quality of Houses, Schools, Public or Private buildings.

Also ensuring the Safety of Health facilities, Public Health Services, Water Supply, Sewerage System etc.

Mitigation complements the Disaster Preparedness and Disaster Response activities.

A Specialised Unit within the National Health Disaster Management Program should coordinate the works of experts in the field of

- Health, Public Policy and Public Health
- Hospital Administration
- Water Systems
- Engineering and Architecture
- Planning, Education etc

The Mitigation Program will direct the following activities

1. Identify areas exposed to Natural Hazards and determine the vulnerability of key health facilities and water systems
2. Coordinate the work of Multi Disciplinary teams in designing and developing building codes and protect the water distribution from damages
3. Hospitals must remain operational to attend to disaster victims
4. Include Disaster Mitigation Measures in the planning and development of new facilities
5. Identify priority hospitals and critical health facilities that complies with current building codes and standards
6. Ensure that mitigation measures are taken into account in a facility's maintenance plans
7. Inform, sensitize and train those personnel's who are involved in planning, administration, operation, maintenance and use of facilities about disaster mitigation
8. Promote the inclusion of Disaster Mitigation in the curricula of Professional training institutes

Technical Health Programs

- Treatment of casualties
- Identification and disposal of bodies
- Epidemiological surveillance and disease control
- Basic sanitation and sanitary engineering

- Health management in shelters or temporary settlements
- Training health personnel and the public
- Logistical resources and support
- Simulation exercises / Mock Exercises
    1. Desktop simulation exercises [war games]
    2. Field exercises
    3. Drills designed to impart skills

Epidemiologic Surveillance and Disease Control

Natural disasters may increase the risk of preventable diseases due to adverse changes in the following areas

- Population density
- Population displacement
- Disruption and contamination of water supply and sanitation services
- Disruption of public health programs
- Ecological changes that favor breeding of vectors
- Displacement of domestic and wild animals
- Provision of emergency food, water and shelter in disaster situation

The principles of preventing and controlling communicable diseases after a disaster are:

- Implement as soon as possible all public health measures to reduce the risk of disease transmission
- Organize a reliable disease reporting system to identify outbreaks and to promptly initiate control measures
- Investigate all reports of disease outbreaks rapidly. Early clarification of the situation may prevent unnecessary dispersion of scarce resources and disruption of normal progress

Environmental Health Management

Post disaster environmental health measures can be divided into two priorities

1. Ensuring that there are adequate amounts of safe drinking water, basic sanitation facilities, disposal of excreta, waste water and solid wastes and adequate shelter

2. Providing food protection measures, establishing or continuing vector control measures, and promoting personal hygiene

- Water Supply

  a) Alternate water sources

  b) Mass distribution of Disinfectants

- Food Safety
- Basic Sanitation and Personal Hygiene
- Solid Waste Management
- Vector Control
- Burial of the Dead
- Public information and the Media

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 disaster preparedness?

.....

.....

.....

.....

2) What are the elements of the disaster response?

.....

.....

.....

.....

3) How should health care facilities prepare for disaster response?

.....

.....

.....

.....

4) What is disaster mitigation?

.....

.....

.....

.....

4.6.5 Rehabilitation

An effective plan for public health and other personnel during a disaster would outline activities designed to minimize the effects of the catastrophe.

These efforts can be summarized as closely **situation analysis and response;** the two types of activities are interrelated.

Although many relief workers may be needed to obtain surveillance information, analyze the data, provide relief services, evaluate results, and provide information to the public, it is essential that a single person with managerial experience be placed in absolute charge of the entire disaster relief operation.

Following a disaster, the desire to provide immediate relief may lead to hasty decisions which are not based on the actual needs of the affected population.

The disaster relief managers can determine the actual needs of the population and make responsible relief decisions.

Reliable information must be obtained on problems occurring in the disaster stricken area, relief resources available and relief activities already in progress. For this, a Surveillance systems must be set up immediately.

The objective of Surveillance in a disaster situation is to obtain information required for making relief decisions.

The specific information required would vary from disaster to disaster, but a basic, three -step processes includes:

(1) Collect data,

(2) Analyze data,

(3) Respond to data.

The analysis involves collating and interpreting the data and can include asking questions as the following:

- What problems are occurring? Why are they occurring?
- Where are problems occurring?
- Who is affected?

- What problems are causing the greatest morbidity and mortality?
- What problems are increasing or decreasing?
- What problems will subside on their own?
- What problems will increase if unattended?
- What relief resources are available?
- Where are relief resources available?
- How can relief resources be used most efficiently?
- What relief activities are in progress?
- Are relief activities meeting relief needs?
- What additional information is needed for decision making?

After answering such questions one can carry out the third part, i.e., planning an appropriate Response to the situation described in the surveillance data.

In developing this plan one will decide what types of relief responses are appropriate and what the relative priorities are among the relief activities.

This 3 step process of Data Collection, Analysis and Response can be described as a closed feedback system involving re-evaluation of relief needs and their effects.

Surveillance following a disaster evolves in three phases

1. Immediate Assessment
2. Short term assessment
3. Ongoing Surveillance

Immediate Assessment

The object of this phase of surveillance is to obtain as much general information as possible and as quickly as possible.

The most basic information needed at this point is the following:

(1) The geographical extent of the disaster-stricken area,

(2) The major problems occurring in the area,

(3) The number of people effected.

This information can be obtained by whatever means seems most efficient. Listening carefully and asking questions is the best way to begin.

An Arial survey may be useful in defining the geographical extent of the disaster-stricken area and in observing major damage and destruction.

Census data can be examined to determine how many people previously lived in the disaster-stricken area and thus were at risk.

Hospitals, clinics, and morgues, which were in operation, may be able to obtain numbers of known deaths and injuries.

It is useful to determine the most frequent causes of deaths and types of injuries in order to predict whether demands for medical care will be increasing or decreasing.

Some problems likely to occur after a disaster can be predicted according to past experience with that particular type of disaster.

For example, experience has shown that disruption of water supplies has often been a problem following earthquakes.

New types of disasters, such as chemical emergencies and nuclear accidents, still present many unknown problems.

Short-term Assessment

The short-term assessment involves more systematic methods of collecting data and is likely to result in more detailed reliable information on problems, relief resources, and relief information on problems, relief resources and relief activities in progress.

One way to organize data collection during this phase of assessment is to divide the disaster-stricken area into smaller areas or "blocks" to be surveyed simultaneously by different workers or teams of workers.

Simple reporting forms can be developed and workers sent out to survey the different areas and report at a specified time.

The following is a list of Information, which may be needed in order to make relief decisions

- The geographical extent of the affected area as defined by streets and other clear boundaries.
- The number of persons known to be dead, possibly according to age groups and sex.
- The estimated number of persons severely injured and / requiring medical care, possibly according to age group, sex, and type of injury or medical problem.
- Estimated number of homes destroyed, homes uninhabitable, and homes, which are still habitable.
- Condition of schools, churches, temples and other public buildings etc.
- Condition and extent of water supply.

- Condition and extent of food supply.
- Condition of roads, bridges, communication facilities and public utilities.
- Location and condition of health facilities
- Estimates of medical personnel, equipment's and supplies available
- Description of relief activities already in progress

  (E.g. search and rescue, first aid, food relief etc).

Ongoing Surveillance

Depending on the factors above, short-term assessment may take as little as 5-6 hours or up to 3-4 days. As early as possible, relief priorities should be determined, resources ordered and full scale relief activities initiated.

Once the short-term assessment is complete and appropriate relief is in progress, surveillance becomes an ongoing system.

When information obtained by the ongoing surveillance is analyzed, new problems may become apparent, requiring investigation.

The surveillance report is one way of coordinating different agencies and preventing duplication of relief efforts.

A relief plan developed during any of the surveillance cycle may include some or all of the following activities:

- Rescue of victims
- Provision of emergency medical care
- Elimination of physical dangers (fire, gas leak etc)
- Evacuation of the population (nuclear and chemical emergencies)
- Provision of preventive and routine medical care
- Provision of water
- Provision of food
- Provision of clothing
- Provision of shelter
- Disposal of human waste
- Control of vector born diseases
- Disposal of human bodies
- Disposal of solid waste

Mass Casualty Management

Management of mass casualties is divided into three main areas:

1. Pre-Hospital Emergency Care
    - Search and Rescue
    - First Aid
    - Field Care
    - Stabilization of the victims
    - Triage
    - Tagging
2. Hospital Reception and Treatment
    - Organizational structure in the hospital with a disaster management team consists of senior officers in the medical, nursing and administrative fields
    - Standardized simple therapeutic procedures followed
3. Re-distribution of Patients between Hospitals

4.6.6 Reconstruction

In the case of disaster management, the Evaluator will be looking at the "actual" **verses the "desired"** on two levels, i.e. the overall outcome of disaster management efforts and the impact of each discrete category of relief efforts (Provision of food, shelter, management of communications etc)

A critical step in the management of any disaster relief is the setting of objectives, which specify the intended outcome of the relief.

The general objectives of the disaster management will be the elimination of unnecessary morbidity, mortality and economic loss directly and indirectly attributable to mismanagement of disaster relief.

The comparison of the "actual" with "desired" is the first critical step of evaluation. If the objectives were met, those who have participated in the relief have demonstrated that they have accomplished what they set out to do.

On the other hand, if the objectives were not met, it is desirable for those conducting the evaluation to continue with the evaluation process, identify the reasons for the discrepancy and suggest corrective action.

Simulated Disaster Preparedness Operations should be undertaken to test the various components before actual need arise.

Evaluation of the health disaster management program

- Evaluation of the preparedness program
- Evaluation of the mitigation measures
- Evaluation of the training

4.7 DISASTER MANAGEMENT AND BUSINESS CONTINUITY PLANNING

4.7.1 Need to Plan for Possible Crisis

It's essential to **plan thoroughly** to protect yourself from the impact of potential crises - from fire, flood or theft to IT system failure, restricted access to premises or illness of key staff.

This planning is very important for small businesses since they often lack the resources to cope easily in a crisis.

Failure to plan could be disastrous. At best you risk losing customers while you're getting your business back on its feet. At worst your business may never recover and may ultimately **cease trading.**

As part of the planning process you should:

- identify potential crises that might affect you
- determine how you intend to minimize the risks of these disasters occurring
- set out how you'll react if a disaster occurs in a business continuity plan
- test the plan regularly

4.7.2 Benefits of a Business Continuity Plan

A carefully thought-out business continuity plan will make coping in a crisis easier and enable you to minimise disruption to the business and its customers.

It will also prove to customers, insurers and investors that your business is robust enough to cope with anything that might be thrown at you - possibly giving you the edge over your competitors or lower insurance premiums.

4.7.3 Assess the Possible Impact of Disaster on Your Business

You need to analyse the probability and consequences of disaster that could affect your business. This involves:

- assessing the likelihood of a particular crisis occurring – and its possible frequency
- determining its possible impact on your operations

This kind of analysis should help you to identify which business functions are essential to day-to-day business operations. You're likely to conclude that certain roles within the business – while necessary in normal circumstances – aren't absolutely critical in a disaster scenario.

4.7.4 Likelihood of Risks Occurring

It can help to grade the probability of a particular disaster or crisis occurring, perhaps on a numerical scale or as high, medium or low.

This will help you to decide your business' attitude towards each risk. You may decide to do nothing about a low-probability disaster - although remember that it could still be highly damaging to your business if it occurred, eg. a terrorist attack.

4.7.5 Potential Impact of a Disaster

To determine the possible impact of a crisis on your business, it can be helpful to think of some of the worst possible scenarios and how they might prove debilitating for the business.

For instance, how could you access data on your customers and suppliers if computer equipment was stolen or damaged by a flood? Where would the business operate from if your premises were destroyed by fire?

It's essential to look at risks from the perspective of your **customers**. Consider how they'd be affected by each potential crisis.

4.7.6 Minimize the Potential Impact of Disaster

Once you have identified the key risks your business faces, you need to take steps to protect your business functions against them.

Premises

Good electrical and gas safety could help protect premises against fire. Installing fire and burglar alarms also makes sense.

Think what you would do in an emergency if your premises couldn't be used. For example, you might suggest an arrangement with another local business to share premises temporarily if a crisis affected either of you.

You may consider using a business continuity supplier, which can make alternative premises available at short notice. But this can be expensive.

Equipment/Machinery

If you use vital pieces of equipment, you may want to cover them with maintenance plans guaranteeing a fast emergency call-out.

IT and Communications

Installing anti-virus software, backing up data and ensuring the right maintenance agreements are in place can all help protect your IT systems. You

might also consider paying an IT company to regularly back up your data offsite on a secure server.

For more information, see our guide on how to keep your systems and data secure.

Printing out copies of your customer database can be a good way of ensuring you can still contact customers if your IT system fails.

People

Try to ensure you're not dependent on a few staff for key skills by getting them to train other people.

Consider whether you could get temporary cover from a recruitment agency if illness left you without several key members of staff. And take health and safety seriously to reduce the risk of staff injuries.

Transport

Document how each member of staff gets to work. Consider establishing a car sharing scheme or providing staff with transport to and from work. Encourage the use of public transport. Provide IT support systems to facilitate home working should the need arise.

Consider stock piling mission critical supplies and materials. Create a list of alternative supplies should your main supplier be unable to deliver the goods and materials you require.

The Department of Energy and Climate Change and the Cabinet Office have produced guidance for businesses on how to draw up a business continuity plan to deal with potential fuel shortages. The guide outlines the possible impact of a fuel shortage and contains measures you could implement in the event of a strike or failure in the fuel supply.

Insurance

Insurance forms a central part of an effective risk-management strategy. For more information see our guides on how to insure your business and assets – general insurances and how to insure your business – people, life and health.

4.7.7 Plan How You'll Deal with an Emergency

You should draw up a business continuity plan setting out in writing how you will cope if a disaster does occur.

It should detail:

- the key business functions you need to get operating as quickly as possible and the resources you'll need to do so

- the roles of individuals in the emergency

Making the most of the **first hour** after an emergency occurs is essential in minimizing the impact. As a result, your plan needs to explain the immediate actions to be taken.

Consider whether you'll need to give staff **specific training** to enable them to fulfill their responsibilities in an emergency situation. Ensure all employees are aware of what they have to do.

Arranging the plan in the form of checklists can be a good way to make sure that key steps are followed.

Include **contact details** for those you're likely to have to notify in an emergency such as the emergency services, insurers, the local council, customers, suppliers, utility companies and neighbouring businesses.

It's also worth including details of service-providers such as glaziers, locksmiths, plumbers, electricians, Doctors and IT specialists. Include maps of your premises' layout to help emergency services, showing fire escapes, sprinklers and other safety equipment.

Set out how you'll deal with possible **media interest** in an incident. Appoint a single company spokesperson to handle questions and try to be positive in any statements you issue. Ensure staff, customers and suppliers are informed before they find out in the media

Finally, make sure hard copies of your business continuity plan are lodged at your home and with your bank and at the homes of other key members of staff.

4.7.8 Test Your Business Continuity Plan

Once your plan is in place, you'll need to test how well it's likely to perform in the event of an emergency.

Although by their nature crises are hard to simulate in a rehearsal, you can assess your plan against a number of possible scenarios in a paper-based exercise.

Think about the things that would cause most disruption and that are most likely to happen to your business. Then make sure that your plan covers each of the risks. Ask yourself the following key questions:

- Does it set out each employee's role in the event of each emergency?
- Have you set out the right steps to take?

Is the order of the plan correct so that priority actions to minimize damage will take place immediately after the incident?

Make some telephone calls to check that the key contacts and phone numbers that you have given are correct. Having to find the right number after a crisis could use up valuable time.

4.7.9 Keep Your Plan Updated

Remember to update your plan regularly to take into account your business changing circumstances.

If you move into new premises, for example, you could face an entirely new set of risks. You'd need to draw up new maps for the emergency services and amend any contact numbers necessary.

You should test your plan regularly, even if your business hasn't undergone significant changes.

4.8 DISASTER SIMULATION EXERCISE

Disaster simulators are the devices which are made for giving an illusion of disaster so that the people of rescue force can get an exercise to prevent people in disaster situations. There are different disaster simulators which gives the feeling of the disaster like

1. **Damage Control Training:** Damage control is a term used in the Merchant Marine, maritime industry and navies for the emergency control of situations that may hazard the sinking of a ship. It is also used in other contexts as explained below. Examples are:

    - rupture of a pipe or hull especially below the waterline and
    - damage from grounding (running aground) or hard berthing against a wharf.
    - temporary fixing of bomb or explosive damage.

Fig. 5

In the episode, teams had to seal leaking water pipes in a flooding mock-up of the interior of a naval ship. So they can find the idea of special buildings that realistically and physically simulate disasters fascinating.

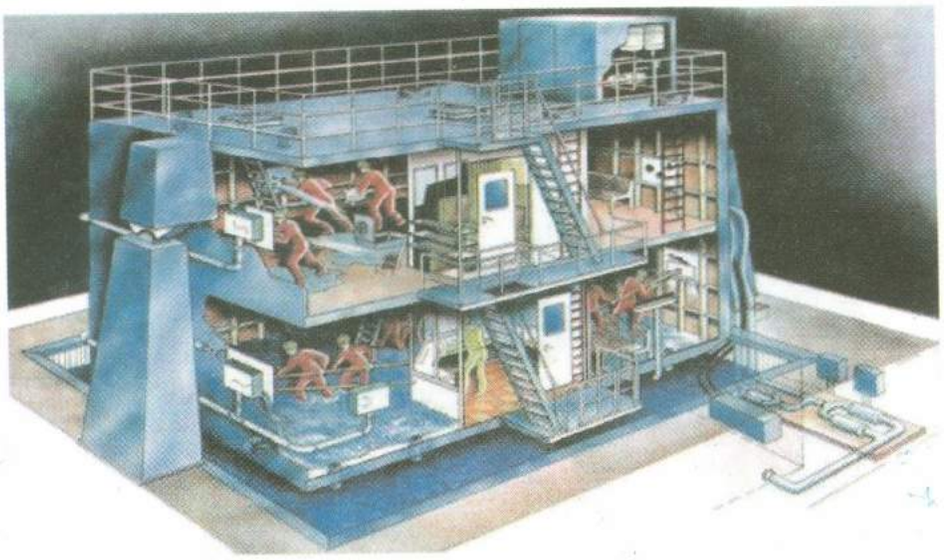

Fig. 6

2. **Submarine escape training tower (SETT):** A **Submarine Escape Training Tower** is part of a facility used for training submariners in methods of emergency escape from a disabled submarine. It is a tall cylinder filled with water with several entrances at varying depths each simulating an airlock in a submarine. Since the 1930s Towers have been built for use by the Royal Navy, US Navy, Royal Australian Navy and in several other countries.

Fig. 7

These towers are 100-feet deep, the tallest diving tanks in the world, and teach students how to escape from a disabled submarine while wearing special evacuation suits.

3. **Fake Airplanes:** Additionally, firefighters have burn buildings and fake airplanes, while police officers have mock towns

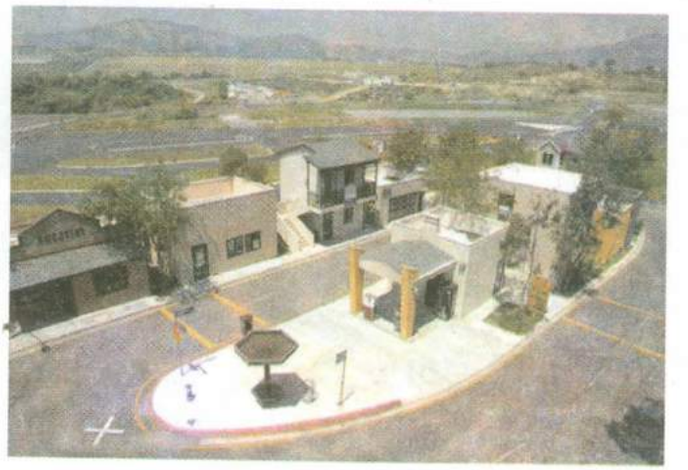

Fig. 8

4.9 CASE STUDY OF DISASTER SIMULATION EXERCISE

Sri Lanka Disaster Simulation Exercise

The Challenge

Sri Lanka was one of the Southeast Asian countries impacted by the December 26, 2004, tsunami. This natural disaster devastated 75 percent of its coastal belt, displaced 44,500 people and left an estimated 3,800 dead.

The Solution

Beginning in 2006, the US Forest Service began delivering Incident Command System (ICS) training as part of a United Nations (UN) initiative titled the Indian Ocean Tsunami Warning System. This comprehensive preparedness effort was designed to enable more effective governmental response to future disasters. During the spring of 2007, the Northeastern Area (NA) participated in the Forest Service International Programs Initiative offering disaster preparedness programs to the Sri Lanka National Disaster Management Centre. As the ICS training was being completed, the Sri Lankan government started preparing to test their new incident management plans and team skills in a full-scale disaster exercise. Meetings with an exercise development team in late March set the stage for conduct of the exercise at the end of June. The Galle District at the southwestern tip of Sri Lanka had been particularly hard hit in the 2004 tsunami and was suggested as the focus for the exercise. A soccer

field near the Police Emergency Communications Center became the Incident Command Post for the exercise, with communication links to the District Secretariat Emergency Operations Center some four kilometers distant. Local police, fire and emergency medical services, public works department employees, environmental spill responders, electric power utility workers, and Sri Lankan Red Cross staff all had roles in the exercise.

Resulting Benefits

With ICS training to enable a managed team response, other UN efforts helped rebuild emergency response infrastructure, tsunami warning systems, and disaster ***response*** plans. NA, acting as a consultant, helped the Sri Lankan incident management team (IMT) creates exercise development and evaluation plans. The resulting 3 ½ hour exercise included 25 simulated disaster inputs, covering mass casualties, interruption of electronic communications, civilian medical and fire emergencies, environmental impacts requiring timely intervention, and civilian evacuations. The exercise tested understanding of ICS within a division-level unit of the Disaster Management workforce and key local cooperators. It helped identify areas to improve the local disaster management response plan and fit it to ICS structures. Overall, the group performed admirably during the exercise.

John Grosman, Northeastern Area fire training officer, and Hiranthe Senaratne of the Sri Lanka Disaster Management Centre go over plans for the exercise. (Photo credit: John Grosman)

Sharing Success

The Sri Lanka Simulation Team facilitated a group discussion with participants at the end of the effort to acknowledge individual success, and identify needed improvements for future emergency response.

Sri Lankan ICS cadre that helped develop the simulation exercise will continue to use Federal Emergency Management Administration exercise design resources in future training.

The group receiving the ICS training will continue developing additional IMTs, while themselves serving key IMT roles in any disaster response, anywhere within the country.

Nepal Simulation: Exercise Khichadi, November 1-8

On October 31, emergency managers and teams from Nepal, Pakistan, India, Bangladesh, and Sri Lanka gathered in Kathmandu for a unique training event: a simulation exercise for a sudden-onset disaster. On November 4, following two days of classroom training, the 30 trainees were given the location of the disaster.

Fig. 10

The exercise scenario directed the teams to a ridge top village called Ravi Opi, approximately 30 km east of Kathmandu. Accompanied by monitors and observers, the teams quickly arranged transportation to the village while beginning operational planning.

Check Your Progress 3

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

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

1) What are the objectives of Surveillance in a disaster situation?

.....

.....

.....

.....

2) What are the activities of the surveillance during relief plan?

.....

.....

.....

.....

3) What do you understand by disaster simulators? Give some examples.

.....

.....

.....

.....

4.10 LET US SUM UP

Disasters have resulted in significant morbidity, mortality and economic loss. Public health is concerned with two objectives in disaster management;

- the elimination of the preventable consequences of the disaster
- The prevention of losses due to disaster mismanagement.

Appropriate disaster relief follows a specific pattern;

- Gathering information on the situation
- Analysis of this information
- Developing and implementing an appropriate response

This pattern occurs at various levels;

- immediate assessment,
- short-term assessment
- ongoing assessment,

Through study of the past disasters, their effects and their relief efforts [what has been effective and what have been mismanaged] better plans are now available for effective disaster management as well as for the reduction of preventable losses.

- The disaster proneness varies widely from State to State.

- The country will have to pay more attention towards creating public awareness and preparedness in respect of people living in known disaster prone areas.
- Special training is required to the medical, paramedical, voluntary workers in the relief and rescue work.
- Any Disaster is an emergency situation and the health sector alone cannot tackle it in isolation.
- It must have Coordination with the local community, civil defense, army, police, fire brigade and with various governmental and non-governmental bodies including voluntary organizations like Red Cross.

4.11 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

1) Disaster is a sudden, calamitous event bringing great damage, loss, and destruction and devastation to life and property. The damage caused by disasters is immeasurable and varies with the geographical location, climate and the type of the earth surface/degree of vulnerability. This influences the mental, socio-economic, political and cultural state of the affected area. Generally, disaster has the following effects in the concerned areas,

   - It completely disrupts the normal day to day life
   - It negatively influences the emergency systems
   - Normal needs and processes like food, shelter, health, etc. are affected and deteriorate depending on the intensity and severity of the disaster.

2)

Major natural disasters: • Flood • Cyclone • Drought • Earthquake	**Minor natural disasters:** • Cold wave • Thunderstorms • Heat waves • Mud slides • Storm
Major manmade disaster: • Setting of fires • Epidemic • Deforestation • Pollution due to prawn cultivation • Chemical pollution. • Wars	**Minor manmade disaster:** • Road / train accidents, riots • Food poisoning • Industrial disaster/ crisis • Environmental pollution

3) The extent of damage in a disaster depends on:

- The impact, intensity and characteristics of the phenomenon and
- How people, environment and infrastructures are affected by that phenomenon

This relationship can be written as an equation:

Government of India [GoI], Ministry of Home Affairs [MHA] and United Nations Development Programme [UNDP] have signed an agreement on August 2002 for implementation of ***"Disaster Risk Management"*** Programme to reduce the vulnerability of the communities to natural disasters, in identified multi–hazard disaster prone areas.

Goal: "Sustainable Reduction in Natural Disaster Risk" in some of the most hazard prone districts in selected states of India".

Check Your Progress 2

1) Disaster preparedness is an ongoing, multi-sectoral activity to carry out the following activities:

- Evaluate the risk of the country or particular region to disasters.
- Adopt standards and regulations
- Organize communication, information and warning systems
- Ensure coordination and response mechanisms
- Adopt measures to ensure that financial and other resources are available for increased readiness and can be mobilized in disaster situations.
- Develop public education programs
- Coordinate information sessions with news media

2) Appropriate application of current technology can prevent much of the death, injury and economic disruption resulting from disasters

Morbidity and mortality resulting from disasters differ according to the type and location of the event.

In any disaster, prevention should be directed towards reducing

- Losses due to the disaster event itself
- Losses resulting from the Mismanagement of disaster relief.

3) To prepare for disaster response, Health care facilities should:

a) Prevent unnecessary morbidity, mortality and economic loss resulting directly from the disaster.

b) Eliminate morbidity, mortality, and economic loss directly attributable to mismanagement of disaster relief efforts.

4) It is virtually impossible to prevent occurrence of most Natural Disasters, but it is possible to minimize or mitigate their damage effects. Mitigation measures aim to reduce the Vulnerability of the System [eg. By improving and enforcing building codes etc]. Disaster prevention implies complete elimination of damages from a hazard, but it is not realistic in most hazards. [eg. Relocating a population from a flood plain or from beach front]. Medical Casualty could be drastically reduced by improving the Structural Quality of Houses, Schools, Public or Private buildings. Also ensuring the Safety of Health facilities, Public Health Services, Water Supply, Sewerage System etc.

Check Your Progress 3

1) The objective of Surveillance in a disaster situation is to obtain information required for making relief decisions.

The specific information required would vary from disaster to disaster, but a basic three step processes includes:

(1) Collect data, (2) Analyze data, (3) Respond to data.

2) A relief plan developed during any of the surveillance cycle may include some or all of the following activities:

- Rescue of victims
- Provision of emergency medical care
- Elimination of physical dangers (fire, gas leak etc)
- Evacuation of the population (nuclear and chemical emergencies)
- Provision of preventive and routine medical care
- Provision of water
- Provision of food
- Provision of clothing
- Provision of shelter
- Disposal of human waste
- Control of vector born diseases
- Disposal of human bodies
- Disposal of solid waste

3) Disaster simulators are the devices which are made for giving an illusion of disaster so that the people of rescue force can get an exercise to prevent people in disaster situations. There are different disaster simulators which gives the feeling of the disaster like Damage Control Training := Damage control is a term used in the Merchant Marine, maritime industry and navies for the emergency control of situations that may hazard the sinking of a ship. It is also used in other contexts as explained below. Examples are:

- rupture of a pipe or hull especially below the waterline and
- damage from grounding (running aground) or hard berthing against a wharf.
- temporary fixing of bomb or explosive damage.

4.12 SUGGESTED READINGS

- *Disaster Management* By G.K. Ghosh, A.P.H. Publishing Corporation
- *Disaster Management - Recent Approaches* By Arvind Kumar, Anmol Publications
- *Encyclopaedia of Disaster Management* By Goel, S. L., Deep & Deep Publications Pvt Ltd

NOTE

Student Satisfaction Survey

ignou THE PEOPLE'S UNIVERSITY

Student Satisfaction Survey of IGNOU Students

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

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

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

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

NOTE

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

ISBN-978-81-266-5716-2