

Business Continuity Planning and Disaster Recovery Planning

Basic Concepts

1. **Business Continuity Planning:** Planning is an activity to be performed before the disaster occurs or it would be too late to plan an effective response. Business continuity covers the following areas: Business Resumption Planning, Disaster Recovery Planning, and Crisis Management.
2. **Developing a Business Continuity Plan:** The methodology for developing a business continuity plan can be sub-divided into eight different phases: Pre-Planning Activities (Business continuity plan Initiation), Vulnerability Assessment and General Definition of Requirements, Business Impact Analysis, Detailed Definition of Requirements, Plan Development, Testing Program, Maintenance Program, Initial Plan Testing and Plan Implementation.
3. **Business Impact Analysis:** Business Impact Analysis (BIA) is essentially a means of systematically assessing the potential impacts resulting from various events or incidents. It enables the business continuity team to identify critical systems, processes and functions, assess the economic impact of incidents and disasters that result in a denial of access to the system, services and facilities, and assess the "pain threshold," that is, the length of time business units can survive without access to the system, services and facilities.
4. **Plan development:** The objective of this phase is to determine the available options and formulation of appropriate alternative operating strategies to provide timely recovery for all critical processes and their dependencies. The recovery strategies may be two-tiered: Business - Logistics, accounting, human resources, etc., and Technical - Information Technology (e.g. desktop, client-server, midrange, mainframe computers, data and voice networks).
 - 4.1 **Types of Plans:** There are various kinds of plans that need to be designed. They include: Emergency Plan, Backup Plan, and Recovery Plan.
5. **Threats and Risk Management:** Various threats, risks and exposures to computer systems are due to: Lack of Confidentiality, Integrity, and Availability, Unauthorized users attempts to gain access to the system and system resources, Disgruntled employees, Hackers and computer crimes, Terrorism and industrial espionage.
6. **Types of Backups:** Full Backup, Differential Backup, Incremental Backup, and Mirror Backup. Security administrators should consider the following backup options: Cold

Site, Hot Site, Warm Site, and reciprocal Agreement.

7. **Backup Redundancy:** Major points are: Multiple backup Media, Off-site Backup, Where to keep the Backups, Media rotation tactics.
8. **Types of backup Media:** The most common types of backup media available on the market today include: Floppy Diskettes, Compact Disks, Tape Drives, Disk Drives, Removable Disks, DAT (Digital Audio Tape) Drives, Optical Jukeboxes, Autoloader TAPE Systems, USB Flash Drive, and Zip Drive.
9. **Insurance:** Policies usually can be obtained to cover the following resources: Equipment, Facilities, Storage Media, Business Interruption, Extra Expenses, Valuable Papers, Accounts receivable, Media Transportation, Malpractice, errors.
 - 9.1 **Kinds of Insurance:** These are of following types: First-party Insurances- Property Damages, First-party Insurances - Business Interruption, Third-party Insurance – General Liability, Third-party Insurance – Directors and Officers.
10. **Testing Methodology:** With good planning a great deal of disaster recovery testing can be accomplished with moderate expenditure. There are four types of tests: Hypothetical, Component, Module, and Full.
11. **Audit Tools and Techniques:** The best audit tool and technique is a periodic simulation of a disaster. Other audit techniques would include observations, interviews, checklists, inquiries, meetings, questionnaires and documentation reviews. These tools and methods may be categorized as: Automated Tools, Internal Control Auditing, Disaster and Security Checklists, and Penetration Testing.

Question 1

Discuss the objectives and goals of Business Continuity planning.

Answer

Objectives and Goals of Business Continuity Planning: The primary objective of a business continuity planning is to enable an organization to survive a disaster and to re-establish normal business operations. In order to survive, the organization must assure that critical operations can resume normal processing within a reasonable time frame. The key objectives of the contingency plan should be to:

- (i) Provide for the safety and well-being of people on the premises at the time of disaster;
- (ii) Continue critical business operations;
- (iii) Minimise the duration of a serious disruption to operations and resources (both information processing and other resources);
- (iv) Minimise immediate damage and losses;
- (v) Establish management succession and emergency powers;

- (vi) Facilitate effective co-ordination of recovery tasks;
- (vii) Reduce the complexity of the recovery effort;
- (viii) Identify critical lines of business and supporting functions.

Therefore, the goals of the business continuity plan should be to:

- (i) Identify weaknesses and implement a disaster prevention program;
- (ii) Minimise the duration of a serious disruption to business operations;
- (iii) Facilitate effective co-ordination of recovery tasks; and
- (iv) Reduce the complexity of the recovery effort

Question 2

What do you understand by the term Disaster? What procedural plan do you suggest for disaster recovery?

Answer

The term disaster can be defined as an incident which jeopardizes business operations and/or human life. It could be due to sabotage (human) or natural. Following is the procedural plans for disaster recovery.

Disaster Recovery Procedural Plan: Normally disaster recovery procedural plan is made when the system is normally working. After visualizing the disaster the action to be taken by different people of the organization are to be documented. This recovery and planning document may include the following areas:

- (i) The conditions for activating the plans, which describe the process to be followed before each plan, are activated.
- (ii) Emergency procedures, which describe the actions to be taken following an incident which jeopardizes business operations and/or human life. This should include arrangements for public relations management and for effective liaison with appropriate public authorities e.g. police, fire, services and local government.
- (iii) Fallback procedures which describe the actions to be taken to move essential business activities or support services to alternate temporary locations, to bring business process back into operation in the required time-scale.
- (iv) Resumption procedures, which describe the actions to be taken to return to normal business operations.
- (v) A maintenance schedule, which specifies how and when the plan will be tested, and the process for maintaining the plan.
- (vi) Awareness and education activities, which are designed to create an understanding of the business continuity, process and ensure that the business continues to be effective.
- (vii) The responsibilities of individuals describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.

6.4 Information Systems Control and Audit

- (viii) Contingency plan document distribution list.
- (ix) Detailed description of the purpose and scope of the plan.
- (x) Contingency plan testing and recovery procedure.
- (xi) List of vendors doing business with the organization, their contact numbers and address for emergency purposes.
- (xii) Checklist for inventory taking and updating the contingency plan on a regular basis.
- (xiii) List of phone numbers of employees in the event of an emergency.
- (xiv) Emergency phone list for fire, police, hardware, software, suppliers, customers, back-up location, etc.
- (xv) Medical procedure to be followed in case of injury.
- (xvi) Back-up location contractual agreement, correspondences.
- (xvii) Insurance papers and claim forms.
- (xviii) Primary computer centre hardware, software, peripheral equipment and software configuration.
- (xix) Location of data and program files, data dictionary, documentation manuals, source and object codes and back-up media.
- (xx) Alternate manual procedures to be followed such as preparation of invoices.
- (xxi) Names of employees trained for emergency situation, first aid and life saving techniques.
- (xxii) Details of airlines, hotels and transport arrangements.

Question 3

Describe the methodology of developing a Business Continuity Plan.

Answer

The methodology for developing a business continuity plan can be sub-divided into eight different phases. The extent of applicability of each of the phases has to be tailored to the respective organisation. The methodology emphasises on the following:

- (i) Providing management with a comprehensive understanding of the total efforts required to develop and maintain an effective recovery plan;
- (ii) Obtaining commitment from appropriate management to support and participate in the effort;
- (iii) Defining recovery requirements from the perspective of business functions;
- (iv) Documenting the impact of an extended loss to operations and key business functions;
- (v) Focusing appropriately on disaster prevention and impact minimisation, as well as orderly recovery;

- (vi) Selecting business continuity teams that ensure the proper balance required for plan development;
- (vii) Developing a business continuity plan that is understandable, easy to use and maintain; and
- (viii) Defining how business continuity considerations must be integrated into ongoing business planning and system development processes in order that the plan remains viable over time.

Question 4

Briefly explain the various types of system's back-up for the system and data together.

Answer

Types of system's Back-ups: When the back-ups are taken of the system and data together, they are called total system's back-up. System back-up may be a full back-up, an incremental back-up or a differential back-up.

- (i) *Full Backup:* Every backup generation contains every file in the backup set. However, the amount of time and space such a backup takes prevents it from being a realistic proposition for backing up a large amount of data. This is the simplest form of backup with a single restoring session for restoring all backed-up files.
- (ii) *Differential Backup:* It contains all the files that have changed since the last full backup. This is in contrast to incremental backup generation, which holds all the files that were modified since the last full or incremental backup. It is faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved.
- (iii) *Incremental Backup:* Only the files that have changed since the last full backup / differential backup / or incremental backup are saved. This is the most economical method, as only the files that changed since the last backup are backed up. This saves a lot of backup time and space. Normally, it is difficult to restore as you have to start with recovering the last full backup, and then recovering from every incremental backup taken since.
- (iv) *Mirror back-up:* It is identical to a full backup, with the exception that the files are not compressed in zip files and they can not be protected with a password. A mirror backup is most frequently used to create an exact copy of the backup data.

Question 5

As a system auditor, what control measures will you check to minimize threats, risks and exposures in a computerized system?

Answer

To minimize threats to the confidentiality, integrity, and availability, of data and computer systems and for successful business continuity, the system auditor should evaluate potential threats to computer systems. Discussed hereunder are various control measures that will be checked by him to minimize threats, risks and exposures in a computerized system:

- (i) Lack of integrity : Control measures to ensure integrity include implementation of security policies, procedures and standards, use of encryption techniques and digital signatures, inclusion of data validation, editing, and reconciliation techniques for inputs, processes and outputs, updated antivirus software, division of job and layered control to prevent impersonation, use of disk repair utility, implementation of user identification, authentication and access control techniques, backup of system and data, security awareness programs and training of employees, installation of audit trails, audit of adequacy of data integrity.
- (ii) Lack of confidentiality: Control measures to ensure confidentiality include use of encryption techniques and digital signatures, implementation of a system of accountability by logging and journaling system activity, development of a security policy procedure and standard, employee awareness and training, requiring employees to sign a non-disclosure undertaking, implementation of physical and logical access controls, use of passwords and other authentication techniques, establishment of a documentation and distribution schedule, secure storage of important media and data files, installation of audit trails, and audit of confidentiality of data.
- (iii) Lack of system availability: Control measures to ensure availability include implementation of software configuration controls, a fault tolerant hardware and software for continuous usage and an asset management software to control inventory of hardware and software, insurance coverage, system backup procedure to be implemented, implementation of physical and logical access controls, use of passwords and other authentication techniques, incident logging and report procedure, backup power supply, updated antivirus software, security awareness programmes and training of employees, installation of audit trails, audit of adequacy of availability safeguards.
- (iv) Unauthorized users attempt to gain access to the system and system resources: Control measures to stop unauthorized users to gain access to system and system resources include identification and authentication mechanism such as passwords, biometric recognition devices, tokens, logical and physical access controls, smart cards, disallowing the sharing of passwords, use of encryption and checksum, display of warning messages and regular audit programs.

Data transmitted over a public or shared network may be intercepted by an unauthorized user, security breaches may occur due to improper use or bypass of available security features, strong identification and authentication mechanisms such as biometric, tokens, layered system access controls, documentation procedures, quality assurance controls and auditing.

- (v) Hostile software e.g. virus, worm, Trojan horses, etc.: Establishment of policies regarding sharing and external software usage, updated anti-virus software with detection, identification and removal tools, use of diskless PCs and workstations, installation of intrusion detection tools and network filter tools such as firewalls, use of checksums, cryptographic checksums and error detection tools for sensitive data, installation of change detection tools, protection with permissions required for the 'write' function.
- (vi) Disgruntled employees: Control measures to include installation of physical and logical access controls, logging and notification of unsuccessful logins, use of disconnect feature on multiple unsuccessful logins, protection of modem and network devices, installation of one time use only passwords, security awareness programs and training of employees, application of motivation theories, job enrichment and job rotation.
- (vii) Hackers and computer crimes: Control measures to include installation of firewall and intrusion detection systems, change of passwords frequently, installation of one time use passwords, discontinuance of use of installed and vendor installed passwords, use of encryption techniques while storage and transmission of data, use of digital signatures, security of modem lines with dial back modems, use of message authentication code mechanisms, installation of programs that control change procedures, and prevent unauthorized changes to programs, installation of logging feature and audit trails for sensitive information.
- (viii) Terrorism and industrial espionage: Control measures to include usage of traffic padding and flooding techniques to confuse intruders, use of encryption during program and data storage, use of network configuration controls, implementation of security labels on sensitive files, usage of real-time user identification to detect masquerading, installation of intrusion detection programs.

Question 6

What are the audit tools and techniques used by a system auditor to ensure that disaster recovery plan is in order? Briefly explain them.

Answer

Audit tools and techniques used by a system auditor to ensure that the disaster recovery plan is in order, are briefly discussed below:

The best audit tool and technique is a periodic simulation of a disaster. Other audit techniques would include observations, interviews, checklists, inquiries, meetings, questionnaires and documentation reviews. These are categorized as follows:

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

6.8 Information Systems Control and Audit

- (ii) Internal Control auditing: This includes inquiry, observation and testing. The process can detect illegal acts, errors, irregularities or lack of compliance for laws and regulations.
- (iii) Disaster and Security Checklists: These checklists are used to audit the system. The checklists should be based upon disaster recovery policies and practices, which form the baseline. Checklists can also be used to verify changes to the system from contingency point of view.
- (iv) Penetration Testing: It is used to locate vulnerabilities to the system.

Question 7

What analysis should be done for understanding the degree of potential loss (such as reputation damage, regulation effects) of an organization? Enumerate the tasks to be undertaken in this analysis. In what ways the information can be obtained for this analysis?

Answer

Business Impact Analysis (BIA) should be done for assessing the potential impacts resulting from various events or incidents. It is intended to help in understanding the degree of potential loss which could occur. It covers not only financial loss but also other losses due to reputation damage, regulatory effects, etc.

For BIA, the following tasks are to be undertaken:

1. Identify organizational risks, and to minimize potential threats that may lead to a disaster.
2. Identify critical business processes.
3. Identify and quantify threats/ risks to critical business processes both in terms of outage and financial impact.
4. Identify dependencies and interdependencies of critical business processes and the order in which they must be restored.
5. Identify the maximum allowable downtime for each business processes.
6. Identify the type and the quantity of resources required for recovery.
7. Determine the impact to the organisation in the event of a disaster, e.g. financial reputation etc.

The information for this analysis can be obtained in many ways, including:

1. Questionnaires,
2. Workshops,
3. Interviews, and
4. Examination of documents.

The BIA Report should be presented to the Steering Committee. This report identifies critical

service functions and the timeframe in which they must be recovered after interruption. The BIA Report should be used as a basis for identifying systems and resources required to support the critical services provided by information processing and other services and facilities.

Question 8

Describe the methodology and phases of developing a business continuity plan?

Answer

Methodology and phases of developing a business continuity plan: The methodology for developing a business continuity plan can be sub-divided into eight different phases. The extent of applicability of each of the phases has to be tailored to the respective organization. The methodology emphasizes on the following:

- Providing management with a comprehensive understanding of the total efforts required to develop and maintain an effective recovery plan;
- Obtaining commitment from appropriate management to support and participate in the effort;
- Defining recovery requirements from the perspective of business functions;
- Documenting the impact of an extended loss to operations and key business functions;
- Focusing appropriately on disaster prevention and impact minimisation, as well as orderly recovery;
- Selecting business continuity teams that ensure the proper balance required for plan development;
- Developing a business continuity plan that is understandable, easy to use and maintain; and
- Defining how business continuity considerations must be integrated into ongoing business planning and system development processes in order that the plan remains viable over time.

The eight phases are:

- (i) Pre-Planning Activities (Business continuity plan Initiation)
- (ii) Vulnerability Assessment and General Definition of Requirements
- (iii) Business Impact Analysis
- (iv) Detailed Definition of Requirements
- (v) Plan Development
- (vi) Testing Program
- (vii) Maintenance Program

(viii) Initial Plan Testing and Plan Implementation

Question 9

Explain the significance of a Business Impact Analysis (BIA) phase on developing a business continuity plan.

Answer

Significance of a Business Impact Analysis (BIA) phase on developing a business continuity plan: The first step in a sensible business continuity process is to consider the potential impact of each type of problem. Business Impact Analysis (BIA) is essentially a means of systematically assessing the potential impacts resulting from various events or incidents. It enables the business continuity team to identify critical systems, processes and functions, assess the economic impact of incidents and disasters that result in a denial of access to the system, services and facilities, and assess the "pain threshold," that is, the length of time business units can survive without access to the system, services and facilities.

The business impact analysis is intended to help understand the degree of potential loss (and various other unwanted effects) which could occur. This will cover not just direct financial loss, but other issues, such as reputation damage, regulatory effects, etc.

The tasks to be undertaken in this phase are enumerated as under:

- Identify organisational risks - This includes single point of failure and infrastructure risks. The objective is to identify risks and opportunities and to minimise potential threats that may lead to a disaster.
- Identify critical business processes.
- Identify and quantify threats/ risks to critical business processes both in terms of outage and financial impact.
- Identify dependencies and interdependencies of critical business processes and the order in which they must be restored.
- Determine the maximum allowable downtime for each business process.
- Identify the type and the quantity of resources required for recovery e.g. tables chairs, faxes, photocopies, safes, desktops, printers, etc.
- Determine the impact to the organisation in the event of a disaster, e.g. financial reputation, etc.

There are a number of ways to obtain this information:

- Questionnaires,
- Workshops,
- Interviews,
- Examination of documents

The BIA Report should be presented to the Steering Committee. This report identifies critical service functions and the timeframe in which they must be recovered after interruption. The BIA Report should then be used as a basis for identifying systems and resources required to support the critical services provided by information processing and other services and facilities.

Question 10

Explain briefly the following terms with respect to business continuity and disaster recovery planning.

- (i) *Emergency plan*
- (ii) *Single points of failure analysis*
- (iii) *First-party insurances*
- (iv) *Cold-site, hot-site and warm-site*

Answer

- (i) **Emergency plan:** The Plan Development phase of the business continuity planning methodology is to determine the available options and formulation of appropriate alternative operating strategies to provide timely recovery for all critical processes and their dependencies.

The recovery strategies may be two-tiered:

- Business - Logistics, accounting, human resources, etc.
- Technical - Information Technology (e.g. desktop, client-server, midrange, mainframe computers, data and voice networks)

Recovery plan components are defined and plans are documented as Emergency plan, Backup-Plan and Recovery Plan. The organization's recovery strategy needs to be developed for the recovery of the core business processes. In the event of a disaster, it is survival and not business as usual.

The emergency plan specifies the actions to be undertaken immediately when a disaster occurs. Management must identify those situations that require the plan to be invoked for example, major fire, major structural damage, and terrorist attack. The actions to be initiated can vary depending on the nature of the disaster that occurs. If an organization undertakes a comprehensive security review program, the threat identification and exposure analysis phases involve identifying those situations that require the emergency plan to be invoked.

When the situation that evokes the plan has been identified the four aspects of the emergency plan must be articulated. First, the plan must show who is to be notified immediately when the disaster occurs - management, police, fire department, medicos, and so on. Second, the plan must show actions to be undertaken, such as shutdown of equipment, removal of files, and termination of power. Third, any evacuation

procedures required must be specified. Fourth, return procedures (e.g., conditions that must be met before the site is considered safe) must be designated. In all cases, the personnel responsible for the actions must be identified, and the protocols to be followed must be specified clearly.

- (ii) **Single points of failure analysis:** The objective is to identify any single point of failure within the organization's infrastructure, in particular the information technology infrastructure. Single point's of failure have increased significantly due to the continued growth in the complexity in the organization's IS environment. This growth has occurred due to changes in technology and customer's demands for new channels in the delivery service and/or products, for example E-Commerce. Organizations have failed to respond to increase in the exposure from single point of failure by not implementing risk mitigation strategies.

One common area of risk from single point of failure is the telecommunication infrastructure. Because of its transparency, this potential risk is often overlooked. While the resiliency of network and the mean average failures of communication devices, e.g. routers, have improved, it is still a single point of failure in an organization that may lead to disaster being declared. To ensure single point failures are identified within the organizations IS architecture at the earliest possible stage, it is essential, as part of any project, a technology risk assessment be performed.

The objectives of risk assessment are to:

- Identify Information Technology risks
- Determine the level of risk
- Identify the risk factors
- Develop risk mitigation strategies

- (iii) **First-party insurances:** The purpose of insurance is to spread the economic cost and the risk of loss from an individual or business to a large number of people. This is accomplished through the use of an insurance policy. Insurance is generally divided into two general classes based upon whether the insured is the injured party. Lawyers call these two divisions first-party and third-party insurance. First-party insurance identifies claims by the policyholder against their own insurance. The most common form of first-party insurance is property damage.

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

First-party Insurances-Business Interruption: If an insured company fails to perform its contractual duties, it may be liable to its customers for breach of contract. One potential cause for the inability to deliver might be the loss of information system, data or communications. Some in business and the insurance industry have attempted to mitigate this by including information technology in business recovery/disaster plans. As a result, there has emerged a robust industry in hot sites for companies to occupy in case of fire, flood, earthquake or other natural disaster. Disaster recovery has become a necessity in the physical world.

(iv) **Cold-site, hot-site and warm-site:** A key element in minimising the threat of a disaster occurring in an organisation is “hardening” the organisation’s infrastructure from potential sources of risk one of it is alternate processing facility arrangements. A security administrator should consider the following backup options:

- **Cold site:** If an organisation can tolerate some downtime, cold-site backup might be appropriate. A cold site has all the facilities needed to install a mainframe system—raised floors, air conditioning, power, communication lines, and so on. The mainframe is not present, it must be provided by the organisation wanting to use the cold site. An organisation can establish its own cold-site facility or enter into an agreement with another organisation to provide a cold-site facility.
- **Hot site:** If fast recovery is critical, an organisation might need hot site backup. All hardware and operations facilities will be available at the hot site. In some cases, software, data and supplies might also be stored there. A hot site is expensive to maintain. They are usually shared with other organisations that have hot-site needs.
- **Warm site:** A warm site provides an intermediate level of backup. It has all cold-site facilities plus hardware that might be difficult to obtain or install. For example, a warm site might contain selected peripheral equipment plus a small mainframe with sufficient power to handle critical applications in the short run.

Question 11

Explain briefly the software and data back-up techniques.

Answer

Software and Data Back-up Techniques: When the back-ups are taken of the system and data together, they are called total system’s back-up. Systems back-up may be a full back-up, an incremental back-up or a differential back-up.

- (i) **Full Back-up:** This is the simplest form of back-up. With a full back-up system, every back-up generation contains every file in the backup set. However, the amount of time and space such a backup takes prevents it from being a realistic proposition for backing up a large amount of data. When it comes to restoring data, this type of backup is the

simplest to use because a single restore session is needed for restoring all back-up files.

- (ii) **Differential Back-up:** A differential backup generation contains all the files that have changed since the last full backup. This is in contrast to incremental backup generation, which holds all the files that were modified since the last full or incremental backup.

Comparing with full back-up, differential back up is obviously faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved.

Restoring from a differential backup is a two-step operation. Restoring from the last full back-up; and then restoring the appropriate differential backup. The downside to using differential backup is that each differential backup will probably include files that were already included in earlier differential backups.

- (iii) **Incremental Backup:** In an incremental backup generation only the files that have changed since the last full backup / differential back up / or incremental backup are saved. This is the most economical method, as only the files that changed since the last backup are backed up. This saves a lot of backup time and space.
- (iv) **Mirror backup:** It is identical to a full backup, with the exception that the files are not compressed in zip files and they cannot be protected with a password. A mirror backup is most frequently used to create an exact copy of the backup data.

Question 12

Explain audit tools and techniques used for disaster recovery plan.

Answer

Audit Tools and Techniques: The best audit tool and technique is a periodic simulation of a disaster. Other audit techniques would include observations, interviews, checklists, inquiries, meetings, questionnaires and documentation reviews. These tools and methods may be categorized as under:

- (i) **Automated Tools:** Automated tools make it possible to review large computer systems for a variety of flaws in a short time period. They can be used to find threats and vulnerabilities such as weak access controls, weak passwords, lack of integrity of the system software etc.
- (ii) **Internal Control Auditing:** This includes inquiry, observation and testing. The process can detect illegal acts, errors, irregularities or lack of compliance of laws and regulations.
- (iii) **Disaster and security checklists:** A checklist can be used against which the systems can be audited. The checklist should be based upon disaster recovery policies and practices, which form the baseline. Checklists can also be used to verify changes to the system from contingency point of view.
- (iv) **Penetration Testing:** Penetration testing can be used to locate vulnerabilities.

Question 13

Describe contents of a disaster recovery and planning document.

Answer

Disaster Recovery Procedural Plan Document: The disaster recovery and planning document may include the following areas:

- .. The conditions for activating the plans, which describe the process to be followed before each plan, are activated.
- .. Emergency procedures, which describe the action to be taken following an incident which jeopardizes business operations and / or human life. This should include arrangements for public relations management and for effective liaison with appropriate public authorities e.g. police, fire, services and local government.
- .. Fallback procedures which describe the actions to be taken to move essential business activities or support services to alternate temporary locations, to bring business process back into operation in the required time-scale.
- .. Resumption procedures, which describe the actions to be taken to return to normal business operations.
- .. A maintenance schedule, which specifies how and when the plan will be tested, and the process for maintaining the plan.
- .. Awareness and education activities, which are designed to create an understanding of the business continuity, process and ensure that the business continues to be effective.
- .. The responsibilities of individuals describing who is responsible for executing which component of the plan. Alternative should be nominated as required.
- .. Contingency plan document distribution list.
- .. Detailed description of the purpose and scope of the plan.
- .. Contingency plan testing and recovery procedure.
- .. List of vendors doing business with the organization, their contact numbers and address for emergency purposes.
- .. Check-list for inventory taking and updating the contingency plan on a regular basis.
- .. List of phone numbers of employees in the event of an emergency.
- .. Emergency phone list for fire, police, hardware, software suppliers, customers, back-up location, etc.
- .. Medical procedure to be followed in case of injury.
- .. Backup location contractual agreement, correspondences.
- .. Insurance papers and claim forms.

6.16 Information Systems Control and Audit

- .. Primary computers Centre hardware, software, peripheral equipment and software configuration.
- .. Location of data and program files, data dictionary, documentation manuals, source and object codes and back-up media.
- .. Alternate manual procedures to be followed such as preparation of invoices.
- .. Names of employees trained for emergency situation, first aid and life saving techniques.
- .. Details of airlines, hotels and transport arrangements.

Question 14

Give objectives and goals of business continuity planning.

Answer

Objectives and Goals of Business Continuity Planning: The primary objective of a business continuity plan is to enable an organization to survive a disaster and to re-establish normal business operations. In order to survive, the organization must assure that critical operations can resume normal processing within a reasonable time frame. The key objectives of the contingency plan should be to:

- (i) Provide for the safety and well-being of people on the premises at the time of disaster;
- (ii) Continue critical business operations;
- (iii) Minimize the duration of a serious disruption to operations and resources (both information processing and other resources);
- (iv) Minimize immediate damage and losses;
- (v) Establish management succession and emergency powers;
- (vi) Facilitate effective coordination of recovery tasks;
- (vii) Reduce the complexity of the recovery effort;
- (viii) Identify critical lines of business and supporting functions;

Therefore, the goals of the business continuity plan should be to:

- (i) Identify weaknesses and implement a disaster prevention program;
- (ii) Minimize the duration of a serious disruption to business operations;
- (iii) facilitate effective coordination of recovery tasks;
- (iv) reduce the complexity of the recovery effort.

Question 15

PQR Enterprises uses business continuity and disaster recovery plans in its various operations. Business continuity focuses on maintaining the operations of the organization,

especially the IT infrastructure in face of a threat that has materialized. Disaster recovery, on the other hand, arises mostly when business continuity plan fails to maintain operations and there is a service disruption. This plan focuses on restarting the operation using a prioritized resumption list.

Read the above carefully and answer the following:

- (a) In your opinion, what should be the goals of a business continuity plan?*
- (b) In the development of a business continuity plan, there are total eight phases; Business Impact Analysis is the third important phase. Discuss various tasks which are to be undertaken in this phase.*
- (c) There are various available backup techniques e.g. Full backup, Incremental backup, Differential backup, and Mirror backup. Describe differential backup technique in detail.*

Answer

- (a)** The goals of the business continuity plan should be to:
 - identify weaknesses and implement a disaster prevention program;
 - minimize the duration of a serious disruption to business operations;
 - facilitate effective co-ordination of recovery tasks; and
 - reduce the complexity of the recovery effort.
- (b)** A number of tasks are to be undertaken in this phase as enumerated under:
 - Identify organizational risks - This includes single point of failure and infrastructure risks. The objective is to identify risks and opportunities and to minimize potential threats that may lead to a disaster.
 - Identify critical business processes.
 - Identify and quantify threats/ risks to critical business processes both in terms of outage and financial impact.
 - Identify dependencies and interdependencies of critical business processes and the order in which they must be restored.
 - Determine the maximum allowable downtime for each business process.
 - Identify the type and the quantity of resources required for recovery e.g. tables chairs, faxes, photocopies, safes, desktops, printers, etc.
 - Determine the impact to the organization in the event of a disaster, e.g. financial reputation, etc.
- (c) Differential Backup:** A differential backup stores files that have changed since the last full backup. Therefore, if a file is changed after the previous full backup, a differential backup takes less time to complete than a full back up. Comparing with full backup,

differential backup is obviously faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved.

Restoring from a differential backup is a two-step operation: Restoring from the last full backup; and then restoring the appropriate differential backup. The downside to using differential backup is that each differential backup will probably include files that were already included in earlier differential backups.

Exercise

Question 1

ABC Company is committed to implement the data backup policy through proper planning. What are the major tips that should be followed by the company for the backup?

Question 2

'With good planning, a great deal of disaster recovery testing can be accomplished with moderate expenditure.' Briefly explain the types of testing techniques.

Question 3

What is Business Continuity Planning? Briefly explain the areas covered by a BCP.

Question 4

A backup plan is to be prepared for XYZ company in order to specify the type of backup to be kept, frequency with which backup is to be undertaken, procedures for making a backup, location of backup resources, site where these resources can be assembled and operations restarted, personnel who are responsible for gathering backup resources and restarting operations, priorities to be assigned to recover various systems, and a time frame for the recovery of each system. But the most difficult part in preparing the backup plan is to ensure that all the critical resources are backed up. List the resources that are to be considered in a backup plan.

Question 5

Briefly explain the control measures to ensure Confidentiality, Integrity, and Availability of data.

Question 6

Differentiate between Incremental Backup and Mirror Backup.

Question 7

Describe various backup devices.