

## **Business Continuity Planning and Disaster Recovery Planning**

### **1. Business Continuity Management:**

- BCM is a very effective management process to help enterprises to manage the disruption of all kinds, providing countermeasures to safeguard from the incident of disruption of all kinds.
- Business continuity means maintaining the uninterrupted availability of all key business resources required to support essential business activities.
- To ensure effective implementation of BCM, the enterprise should conduct regular internal audits at planned intervals.
- BCM facilitates the understanding of the concept, planning, implementation and continuous improvements of BCPs.

#### **Need of BCM**

- BCM ensure continuity of services and operations, an enterprise shall adapt and follow well-defined and time-tested plans and procedures,
- BCM build redundancy in teams and infrastructure, manage a quick and efficient transition to the backup arrangement for business systems and services.

#### **Key terms relating to BCM are:**

- **Business Contingency:** A business contingency is an event with the potential to disrupt computer operations, thereby disrupting critical mission and business functions. Such an event could be a power outage, hardware failure, fire, or storm. If the event is very destructive, it is often called a disaster.
- **BCP Process:** BCP is a process designed to reduce the risk to an enterprise from an unexpected disruption of its critical functions, both manual and automated ones, and assure continuity of minimum level of services necessary for critical operations.
- **Business Continuity Planning (BCP):** It refers to the ability of enterprises to recover from a disaster and continue operations with least impact.

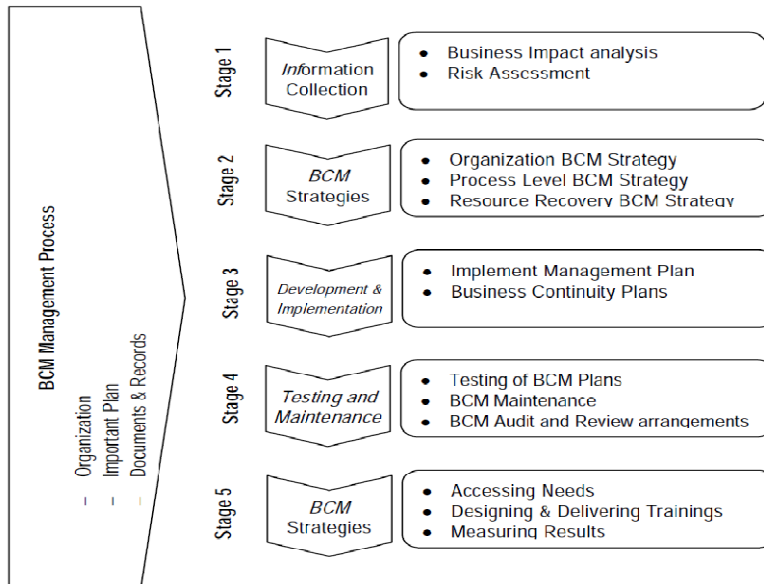
#### **BCM Policy:**

- ✓ BCM policy document is a high level document, which shall be the guide to make a systematic approach for disaster recovery.
- ✓ When developing BCM policy:
  - Organization consider the scope
  - BCM principles,
  - BCM guidelines
  - Minimum standards for the organization.
- ✓ They should refer any relevant standards, regulations or policies that have to be included or can be used as a benchmark.
- ✓ BCM policy defines the processes of setting up activities for establishing a business continuity capability and the ongoing management and maintenance of the business continuity capability.

#### **The objective of this policy is to provide a structure through which:**

- Critical services and activities undertaken by the enterprise operation for the customer will be identified.
- Plans will be developed to ensure continuity of key service delivery following a business disruption
- Invocation of incident management and business continuity plans can be managed.
- Incident Management Plans & Business Continuity Plans are subject to ongoing testing, revision and update.
- Planning and management responsibility are assigned to a member of the relevant senior management team.

## Components of BCM Process



|                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1. BCM Management Process</b>                     | <ul style="list-style-type: none"> <li>The management process enables the business continuity, capacity and capability to be established and maintained.</li> <li>The capacity and capability are established in accordance to the requirements of the enterprise.</li> <li>A BCM process should be in place to address the policy and objectives as defined in the business continuity policy by providing organization structure with responsibilities and authority, implementation and maintenance of business continuity management.</li> </ul> |
| <b>2. BCM Information Collection Process</b>         | <ul style="list-style-type: none"> <li>The activities of assessment process do the prioritization of an enterprise's products and services &amp; the urgency of the activities that are required to deliver them.</li> <li>The pre-planning phase of Developing the BCP also involves collection of information.</li> <li>It enables us to refine the scope of BCP and the associated work program;</li> </ul>                                                                                                                                       |
| <b>3. BCM - Strategy Process</b>                     | <ul style="list-style-type: none"> <li>Finalization of business continuity strategy requires assessment of a range of strategies.</li> <li>This requires an appropriate response to be selected at an acceptable level and during &amp; after a disruption within an acceptable timeframe for each product or service.</li> </ul>                                                                                                                                                                                                                    |
| <b>4. BCM Development and Implementation Process</b> | Development of a management framework and a structure of incident management, business continuity and business recovery and restoration plans.                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>5. BCM Testing and Maintenance Process</b>        | <ul style="list-style-type: none"> <li>BCM testing, maintenance and audit testing in the enterprise BCM to prove the extent to which its strategies and plans are complete</li> <li>A BCP tested periodically because there will be no doubt in the plan and its implementation.</li> <li>The BCM maintenance process demonstrates the documented evidence of the proactive management and governance of the enterprise's business continuity program.</li> </ul>                                                                                    |
| <b>6. BCM Training Process</b>                       | <ul style="list-style-type: none"> <li>Extensive trainings in BCM framework</li> <li>Incident management,</li> <li>Business continuity</li> <li>Business recovery</li> <li>Restoration plans and it Enable it to become part of the enterprise's core values and provide confidence in all stakeholders.</li> </ul>                                                                                                                                                                                                                                  |

**Note: for detail refer Module**

**2. Business Continuity** means maintaining the uninterrupted availability of all key business resources required to support essential business activities.

#### Scope of Business Continuity

- ✓ Top management of the enterprise needs to define the scope of the BCM program
- ✓ It involves identifying the key products and services that support the enterprise's objectives, obligations and statutory duties in line with the threat scenario and the business impact analysis.
- ✓ In case of an outsourced service or activity, the risk accountability remains with the enterprise.

Advantage of Business Continuity - The advantages of BCM are that the enterprise:

- Ability to proactively assess the threat scenario and potential risks;
- Planned response to disruptions which can contain the damage and minimize the impact on the enterprise; and
- Ability to demonstrate a response through a process of regular testing and trainings.

#### **3. Business Continuity Planning:**

- Business Continuity Planning (BCP) is the creation and validation of a practical logistical plan for how an enterprise will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption.
- The logistical plan is called a business continuity plan.
- Planning is an activity to be performed before the disaster occurs otherwise it would be too late to plan an effective response.
- An integrated set of procedures and resources information that is used to recover from disaster that has caused a disruption to business operations. BCP is an ongoing process....not a project.
- The resulting outage from such a disaster can have serious effects on the viability of a firm's operations, profitability, quality of service, and convenience.
- What BCP does: Upon the declaration of a disaster, it activates pre-approved policies and authorities. Restores the outflow of services with least possible impact and cost to the organization.

#### **Objectives of Business Continuity Planning**

primary objective of BCP is to minimize loss by minimizing the cost associated with disruptions and 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: [SCI MME FR]

- Provide the safety and well-being of people on the premises at the time of disaster;
- Continue critical business operations;
- Identify critical lines of business and supporting functions.
- Minimize the duration of a serious disruption to operations and resources (both information processing and other resources);
- Minimize immediate damage and losses;
- Establish management succession and emergency powers;
- Facilitate effective co-ordination of recovery tasks;
- Reduce the complexity of the recovery effort; and

**Goals of the business continuity plan should be to:** [IMFR]

- 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.

Business continuity covers the following areas:

- **Business Resumption Planning:** This is the operation's piece of business continuity planning.
- **Disaster Recovery Planning:** This is the technological aspect of business continuity planning, the advance planning and preparation necessary to minimize losses and ensure continuity of critical business functions of the organization in the event of disaster.
- **Crisis Management:** This is the overall co-ordination of an organization's response to a crisis in an effective timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation or ability to operate.

**BCP Manual:** A BCP manual is

- a documented description of actions to be taken,
  - resources to be used and
  - procedures to be followed before, during and after an event that severely disrupts all or part of the business operations.
- 
- Successful organizations have a comprehensive BCP Manual, which ensures process readiness, data and system availability to ensure business continuity.
  - The BCP Manual is expected to specify the responsibilities of the BCM team, whose mission is to establish appropriate BCP procedures to ensure the continuity of enterprise's critical business functions.
  - BCM Team serves as liaising teams between the functional area(s) affected and other departments providing support services in the event of disaster/ incident.

The BCP is expected to provide:

- reasonable assurance to senior management of enterprise about the capability of the enterprise to recover from any unexpected incident or disaster affecting business operations and continue to provide services with minimal impact.
- Anticipate various types of incident or disaster scenarios and outline the action plan for recovering from the incident or disaster with minimum impact and ensuring 'Continuous availability of all key services to clients'.

#### **4 Developing a Business Continuity Plan**

The methodology for developing a BCP 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 minimization, 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 given as follows:

- (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

*Each of these phases are described below:*

**Phase 1 – Pre-Planning Activities (Project Initiation):** This Phase is used to obtain an understanding of the existing and projected computing environment of the organization.

This enables the project team to:

- ✓ refine the scope of the project and the associated work program;
- ✓ develop project schedules; and
- ✓ identify and address any issues that could have an impact on the delivery and the success of the project.

During this phase, a Steering Committee should be established. The committee should have the overall responsibility for providing direction and guidance to the Project Team. The committee should also make all decisions related to the recovery planning effort. The Project Manager should work with the Steering Committee in finalizing the detailed work plan and developing interview schedules for conducting the Security Assessment and the Business Impact Analysis.

Two other **key deliverables** of this phase are:

- ✓ The development of a policy to support the recovery programs; and
- ✓ An awareness program to educate management and senior individuals who will be required to participate in the project.

**Phase 2 – Vulnerability Assessment and General Definition of Requirements:**

Security and controls within an organization are continuing concern. It is preferable from the an economic and business strategy perspective, to concentrate on activities that have the effect of reducing the possibility of disaster occurrence, rather than concentrating primarily on minimizing impact of an actual disaster. This phase addresses measures to reduce the probability of occurrence.

This phase will include the following **key tasks**:

- ✓ A thorough Security Assessment of the computing and communications environment including personnel practices; physical security; operating procedures; backup and contingency planning; systems development and maintenance; database security; data and voice communications security; systems and access control software
- ✓ security; insurance; security planning and administration; application controls; and personal computers.
- ✓ The Security Assessment will enable the project team to improve any existing emergency plans and disaster prevention measures and to implement required emergency plans and disaster prevention measures where none exist.
- ✓ Present findings and recommendations resulting from the activities of the Security Assessment to the Steering Committee so that corrective actions can be initiated in a timely manner.
- ✓ Define the scope of the planning effort.
- ✓ Analyze, recommend and purchase recovery planning and maintenance software required to support the development of the plans and to maintain the plans current following implementation.
- ✓ Develop a Plan Framework.
- ✓ Assemble Project Team and conduct awareness sessions.

**Phase 3 – Business Impact Assessment (BIA):** A Business Impact Assessment (BIA) of all business units that are part of the business environment enables the project team to:

- ✓ identify critical systems, processes and functions;
- ✓ assess the economic impact of incidents and disasters that result in a denial of access to systems services and other services and facilities; and
- ✓ assess the "pain threshold," that is, the length of time business units can survive without access to systems, services and facilities.

The BIA Report should be presented to the Steering Committee. This report identifies critical service functions and the timeframes 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.

**Phase 4 – Detailed Definition of Requirements:**

During this phase, a profile of recovery requirements is developed. This profile is to be used as a basis for analyzing alternative recovery strategies. The profile is developed by identifying resources required to support critical functions identified in Phase 3. This profile should include hardware (mainframe, data and voice communications and personal computers), software (vendor supplied, inhouse developed, etc.), documentation (DP, user, procedures), outside support (public networks, DP services, etc.), facilities (office space, office equipment, etc.) and personnel for each business unit. Recovery Strategies will be based on short term, intermediate term and long term outages. Another key deliverable of this phase is the definition of the plan scope, objectives and assumptions.

**Phase 5 – Plan Development:**

During this phase, recovery plans components are defined and plans are documented. This phase also includes the implementation of changes to user procedures, upgrading of existing data processing operating procedures required to support selected recovery strategies and alternatives, vendor contract negotiations (with suppliers of recovery services) and the definition of Recovery Teams, their roles and responsibilities. Recovery standards are also be developed during this phase.

**Phase 6 – Testing/Exercising Program:** The plan Testing/Exercising Program is developed during this phase. Testing/exercising goals are established and alternative testing strategies are evaluated. Testing strategies tailored to the environment should be selected and an on-going testing program should be established.

**Phase 7 – Maintenance Program:** Maintenance of the plans is critical to the success of an actual recovery. The plans must reflect changes to the environments that are supported by the plans. It is critical that existing change management processes are revised to take recovery plan maintenance into account. In areas, where change management does not exist, change management procedures will be recommended and implemented. Many recovery software products take this requirement into account.

**Phase 8 – Initial Plan Testing and Implementation:** Once plans are developed, initial tests of the plans are conducted and any necessary modifications to the plans are made based on an analysis of the test results. Specific activities of this phase include the following:

- ✓ Defining the test purpose/approach;
- ✓ Identifying test teams;
- ✓ Structuring the test;
- ✓ Conducting the test;
- ✓ Analyzing test results; and
- ✓ Modifying the plans as appropriate.

The approach taken to test the plans depends in large part, on the recovery strategies selected to meet the recovery requirements of the organization. As the recovery strategies are defined, specific testing procedures should be developed to ensure that the written plans are comprehensive and accurate.

## **4.5.Types of Plans**

There are various kinds of plans that need to be designed. These plans include the following plan:

### **1. Emergency Plan**

- o In emergency plan the actions to be taken immediately when a disaster occurs. Management must identify those situations that require the plan to be invoked.
- o Example :-
  - major fire
  - major structural damage
  - terrorist attack.
- o The actions are depending on the nature of the disaster occurs.

### **2. Back-up Plan**

- o In backup plan, the type of backup to be kept:
  - frequency with which backup is to be taken
  - procedures for making backup
  - location of backup resources
- o allocate the site where these resources can be assembled and operations restarted,
- o procedures specified in the backup plan is to be straightforward.
- o The backup plan needs continuous updating as changes occurs.

### **3. Recovery Plan**

- o Recovery plans set out procedures to restore full information system capabilities.
- o Recovery plan identify a recovery committee who will be responsible for working out the specifics of the recovery to be taken.
- o The plan should specify the responsibilities of the committee and it provide guidelines on priorities to be followed.
- o The plan also indicate which applications are to be recovered first and last.

### **4. Test Plan**

- o The final and last component of a disaster recovery plan is a test plan.
- o The purpose of the test plan is to identify the weakness in the emergency, backup, or recovery plans.
- o They also identify in the preparedness of an organization and its personnel for facing a disaster.

## **4.6. Backup**

- It is a utility program.
- If original database is destroyed then same can be restored with the backup of that database.
- It is create for security purpose

When the back-ups are taken of the system and data together, they are called total system's back-up. Various types of back-ups are given as follows:

• **Full Backup:** A full backup captures all files on the disk or within the folder selected for backup. With a full backup system, 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.

• **Incremental Backup:** An incremental backup captures files that were created or changed since the last backup, regardless of backup type. 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, incremental backup are very difficult to restore. One will have to start with recovering the last full backup, and then recovering from every incremental backup taken since.

• **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 backup. 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 probably includes files that were already included in earlier differential backups.

• **Mirror back-up:** A mirror backup 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.

### **4.6.3. Alternate Processing Facility Arrangements**

Security administrators should consider the following backup options:

#### **(i) Cold Site**

- o 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. An organisation can establish its own cold-site facility or enter into an agreement with another organisation to provide a cold-site facility.
- o Equipment and resource **must be installed** to duplicate the critical business function of an organization.
- o If an organisation can tolerate some downtime, cold-site backup is appropriate.
- o A cold site has all the facilities needed to install a mainframe system—raised floors, air conditioning, power, communication lines etc.

#### **(ii) Warm site**

- o A warm site provides an intermediate level of backup. It has all cold-site facilities in addition to the 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.
- o It is between cold site and hot site.
- o It is better than cold site and less than hot site.
- o It has all cold-site facilities in addition to the hardware that might be difficult to install.
- o They can be either share (sharing server equipment or dedicated own server).

#### **(iii) Hot site**

- o If fast recovery is critical, an organisation need hot site backup.
- o Hot sites are fully equipped with equipment and resources (i.e. All hardware and operations facilities will be available at the hot site) to recover business functions.
- o In some cases, software, data and supplies might also be stored there. They are usually shared with other organisations that have hot-site needs.
- o Most robust disaster recovery technique
- o Most expensive but provide almost zero downtime.

#### **(iv) Reciprocal agreement:**

- o Two or more organisations might agree to provide backup facilities to each other in the event of one suffering a disaster.
- o This backup option is relatively cheap, but each participant must maintain sufficient capacity to operate another's critical system.



If a third-party site is to be used for backup and recovery purposes, security administrators must ensure that a contract is written to cover issues such as

- ✓ how soon the site will be made available subsequent to a disaster;
- ✓ the number of organizations that will be allowed to use the site concurrently in the event of a disaster;
- ✓ the priority to be given to concurrent users of the site in the event of a common disaster;
- ✓ the period during which the site can be used;
- ✓ the conditions under which the site can be used;
- ✓ the facilities and services the site provider agrees to make available; and
- ✓ what controls will be in place and working at the off-site facility.

These issues are often poorly specified in reciprocal agreements. Moreover, they can be difficult to enforce under a reciprocal agreement because of the informal nature of the agreement.

#### 4.16 Disaster Recovery Procedural Plan

The disaster recovery planning document may include the following areas:

##### [ PLANNER C<sup>3</sup>FD BIMA MR.DELL ]

- o Primary computer centre hardware, software, peripheral equipment and software configuration.
- o List of vendors doing business with the organization, their contact numbers and address for emergency purposes.
- o Alternate manual procedures to be followed such as preparation of invoices.
- o Names of employees trained for emergency situation, first aid and life saving techniques.
- o Emergency phone list for fire, police, hardware, software, suppliers, customers, back-up location, etc. The conditions for activating the plans, which describe the process to be followed before each plan, are activated.
- o Resumption procedures, which describe the actions to be taken to return to normal business operations.
  
- o Contingency plan document distribution list.
- o Contingency plan testing and recovery procedure.
- o Checklist for inventory taking and updating the contingency plan on a regular basis.
- o 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.
- o Detailed description of the purpose and scope of the plan.
  
- o Back-up location contractual agreement, correspondences.
- o Insurance papers and claim forms.
- o Medical procedure to be followed in case of injury.
- o 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.
- o Maintenance schedule, which specifies 'how and when the plan will be tested', and the process for maintaining the plan.
- o Responsibilities of individuals describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.
- o Details of airlines, hotels and transport arrangements.
- o 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 liaisoning with appropriate public authorities e.g. police, fire, services and local government.
- o Location of data and program files, data dictionary, documentation manuals, source and object codes and back-up media.
- o List of phone numbers of employees in the event of an emergency.

#### **4.17 Audit of the BCP/DRP**

In a BCP Audit, the auditor is expected to evaluate the processes of developing and maintaining documented, communicated, and tested plans for continuity of business operations and IS processing in the event of a disruption. The objective of BCP audit is to assess the ability of the enterprise to continue all critical operations during a contingency and recover from a disaster within the defined critical recover time period. BCP Auditor is expected to identify residual risks, which are not identified and provide recommendations to mitigate them. The plan of action for each type of expected contingency and its adequacy in meeting contingency requirements is also assessed in a BCP audit.

Sample list of BCP Audit steps are given below:

(i) Determine if a disaster recovery/business resumption plan exists and was developed using a sound methodology that includes the following elements:

- Identification and prioritization of the activities, which are essential to continue functioning.
- The plan is based upon a business impact analysis that considers the impact of the loss of essential functions.
- Operations managers and key employees participated in the development of the plan.
- The plan identifies the resources that will likely be needed for recovery and the location of their availability.
- The plan is simple and easily understood so that it will be effective when it is needed.
- The plan is realistic in its assumptions.

(ii) Determine if information backup procedures are sufficient to allow for recovery of critical data.

(iii) Determine if a test plan exists & to what extent the disaster recovery/business resumption plan has been tested.

(iv) Determine if resources have been made available to maintain the disaster recovery/ business resumption plan and keep it current.

(v) Obtain and review the existing disaster recovery/ business resumption plan.

(vi) Obtain & review plans for disaster recovery/ business resumption testing & documentation of actual tests

(vii) Obtain and review the existing business impact analysis.

(viii) Gather background information to provide criteria and guidance in the preparation and evaluation of disaster recovery/ business resumption plans.

(ix) Determine if copies of the plan are safeguarded by off-site storage.

(x) Gain an understanding of the methodology used to develop the existing disaster recovery/ business resumption plan. Who participated in the development effort?

(xi) Gain an understanding of the methodology used to develop the existing business impact analysis.

(xii) Determine if recommendations made by the external firm who produced the business impact analysis have been implemented or otherwise addressed.

(xiii) Have resources been allocated to prevent the disaster recovery/ business resumption plan from becoming outdated and ineffective?

(xiv) Determine if the plan is dated each time that it is revised so that the most current version will be used if needed.

(xv) Determine if the plan has been updated within past 12 months.

(xvi) Determine all the locations where the disaster recovery/ business resumption plan is stored. Are there a variety of locations to ensure that the plan will survive disasters and will be available to those that need them?

(xvii) Review information backup procedures in general. The availability of backup data could be critical in minimizing the time needed for recovery.

(xviii) Interview functional area managers or key employees to determine their understanding of the disaster recovery/ business resumption plan. Do they have a clear understanding of their role in working towards the resumption of normal operations?

- Does the disaster recovery/ business resumption plan include provisions for Personnel
- Have key employees seen the plan & are all employees aware that there is such a plan? ii) Have employees been told their specific roles and responsibilities if the disaster recovery/ business resumption plan is put into effect?
- Does the disaster recovery/ business resumption plan include contact information of key employees, especially after working hours?
- Does the disaster recovery/ business resumption plan include provisions for people with special needs?
- Does the disaster recovery/ business resumption plan have a provision for replacement staff when necessary?

*(xix) Building, Utilities and Transportation*

- Does the disaster recovery/ business resumption plan have a provision for having a building engineer inspect the building and facilities soon after a disaster so that damage can be identified and repaired to make the premises safe for the return of employees as soon as possible?
- Does the disaster recovery/business resumption plan consider the need for alternative shelter, if needed? Alternatives in the immediate area may be affected by the same disaster.
- Review any agreements for use of backup facilities.
- Verify that the backup facilities are adequate based on projected needs (telecommunications, utilities, etc.). Will the site be secure?
- Does the disaster recovery/ business resumption plan consider the failure of electrical power, natural gas, toxic chemical containers, and pipes?
- Are building safety features regularly inspected and tested? Does the plan consider the disruption of transportation systems? This could affect the ability of employees to report to work or return home. It could also affect the ability of vendors to provide the goods needed in the recovery effort.

*(xx) Information Technology*

- Determine if the plan reflects the current IT environment.
- Determine if the plan includes prioritization of critical applications and systems.
- Determine if the plan includes time requirements for recovery/availability of each critical system, and that they are reasonable.
- Does the disaster recovery/business resumption plan include arrangements for emergency telecommunications?
- Is there a plan for alternate means of data transmission if the computer network is interrupted? Has the security of alternate methods been considered?
- Determine if a testing schedule exists and is adequate (at least annually). Verify the date of the last test. Determine if weaknesses identified in the last tests were corrected.

*(xxi) Administrative Procedures*

- Does the disaster recovery/ business resumption plan cover administrative and management aspects in addition to operations? Is there a management plan to maintain operations if the building is severely damaged or if access to the building is denied or limited for an extended period of time?
- Is there a designated emergency operations center where incident management teams can coordinate response and recovery?
- Determine if the disaster recovery/ business resumption plan covers procedures for disaster declaration, general shutdown and migration of operations to the backup facility.
- Have essential records been identified? Do we have a duplicate set of essential records stored in a secure location?
- To facilitate retrieval, are essential records separated from those that will not be needed immediately?

*(xxii) Does the disaster recovery/ business resumption plan include the names and numbers of suppliers of essential equipment and other material?*

*(xxiii) Does the disaster recovery/ business resumption plan include provisions for the approval to expend funds that were not budgeted for the period? Recovery may be costly.*

*(xxiv) Has executive management assigned the necessary resources for plan development, concurred with the selection of essential activities and priority for recovery, agreed to back-up arrangements and the costs involved, and are prepared to authorize activation of the plan should the need arise.*