

Business Continuity Planning

&

Disaster Recovery Planning

OBJECTIVES

- To equip an IS Auditor with knowledge necessary to evaluate an organization's ability to withstand a variety of emergencies
 - Evaluation tasks typically include an assessment of adequacy of provisions for:
 - ✓ Resumption of normal operations in the event of short term disruptions of IP
 - ✓ Continued availability of IP in the event of primary facilities not being available
 - ✓ Continuity of business in the event of disastrous interruption
-

BUSINESS CONTINUITY PLAN

- BCP is a process designed to:
 - ✓ Minimize the impact of disastrous disruption of IP facilities on critical business operations
 - ✓ Facilitate rapid resumption of critical business operations to an acceptable level of service
 - It is an 'after the fact' process.
 - *It includes a plan (DRP) of actions to be taken before, during and after a disruptive event causing a significant loss of IP resources*
 - It is a responsibility of senior management. Increasingly the trend is to hold senior management liable for failure of 'due care' in disasters.
-

BUSINESS CONTINUITY PLAN

- End user involvement is vital at every stage of BCP process.
- The objective of BCP is not just to develop a plan but to acquire a permanent, ongoing capability.



DISASTERS AND OTHER DISRUPTIVE EVENTS

- Unplanned interruption of normal business process.
 - Disruptive events lasting longer than an acceptable period of time are termed as disaster.
 - These disruptive events stops an organization from providing its critical services caused by the absence of critical resources.
 - The critical resources could be:
 - ✓ People and skill sets
 - ✓ Facilities
 - ✓ Communications
 - ✓ Power (Nearly one-third of all disruptions are caused by loss of power.)
 - ✓ Data/Information
 - ✓ Information Systems
-

DISASTERS AND OTHER DISRUPTIVE EVENTS

- A disaster is described as catastrophic if it involve destruction of the whole or a significant part of IP facilities.
 - Not all disruptions can be called as disaster. Only those that relate to critical business process are covered under the definition of disaster.
 - Examples include:
 - ✓ Earthquakes, storms, floods and fires due to acts of nature
 - ✓ Power outage or other utility failures such as telecommunication, natural gas or other delivery services
 - ✓ Bombings sabotage and internal attacks
 - ✓ Strikes and job actions
 - ✓ System malfunctions, accidental file deletion, denial of service, intrusions, viruses etc.,
-

DISASTER RECOVERY PLAN

- DRP is a set of procedures, to be followed in the event of substantial loss of IP capability, for
 - ✓ Responding to an emergency
 - ✓ Providing extended back up operations during interruptions
 - ✓ Managing recovery and salvage process afterwards
 - **A DRP comprise of four parts viz.**
 - ✓ **Emergency plan**
 - ✓ **Backup plan**
 - ✓ **Recovery Plan**
 - ✓ **Test plan**
-

EMERGENCY PLAN

- Specifies the actions to be taken immediately after the disaster has occurred. Type of action may vary depending upon the nature of disaster. Some disaster may require that all persons leave the place immediately where as others may require few people to stay back to sound alarms, shut down equipment etc.,
 - An emergency plan should include
 - ✓ Lists of persons to be notified
 - ✓ Procedures for evacuation of personnel
 - ✓ Actions to be undertaken for minimizing the loss
 - ✓ Return procedure
-

BACKUP PLAN

- Specifies the resources required to restore IS operations quickly
 - Should include the following:
 - ✓ Location of backup facility
 - ✓ Name, address and contact details of backup team members
 - ✓ HW, SW , data, supplies etc
 - ✓ Priority ranking of systems
 - ✓ Time frame of recovery
 - Should be updated periodically to reflect the changes in operating environment.
-

RECOVERY PLAN

- Should include full details of recovery team including name address and contact details of the team members
 - Should provide guidance on fixing recovery priority
 - Should focus on restoration of full capabilities within shortest possible time
-

TEST PLAN

- Should lay down the testing methodology of emergency, backup and recovery plans with a view to identify the deficiencies, if any
 - Should provide guidance on analysis of test results and responsibility for follow up actions to be taken.
-

COMPONENTS OF BCP

- **Components of a BCP include:**
 - ✓ **Key decision making personnel**
 - ✓ **Back of required supplies**
 - ✓ **Organization and assignment of responsibilities**
 - ✓ **Telecommunication networks**
 - ✓ **Insurance**
 - Copies of BCP should be kept offsite, possibly at homes of key decision making personnel.
-

KEY DECISION MAKING PERSONNEL

- The plan should include a *directory of people who should be notified* in the event of a disaster along with the following:
 - ✓ Prioritized list of contacts
 - ✓ Primary and emergency telephone numbers and address of each critical contact person
 - ✓ Phone number and address of:
 - o Equipment and software vendors
 - o Companies designated to provide supplies and equipment or services
 - o Contact persons at recovery facilities
-

KEY DECISION MAKING PERSONNEL

- o Contact persons at off site media storage facilities
 - o Contact persons authorized to retrieve media from off site facilities
 - o Insurance company
 - o Placement agencies
-

BACKUP OF REQUIRED SUPPLIES

- The plan should include all necessary supplies including the following:
 - ✓ Instructions manual written in simplified manner for use by contract persons involved in the recovery effort
 - ✓ Pre printed stationery including checks, invoices, order forms etc.,
 - ✓ Specialized hardware or software if any
-

ORGANIZATION AND ASSIGNMENT OF RESPONSIBILITIES

- Disaster handling calls for a large number of activities to be performed within a short span of time under not best of the conditions. It is therefore essential that roles are clearly defined and specifically assigned to individuals.
 - Ideally, the following teams should be put into place:
 - ✓ Emergency action team - first response team. Primary focus is to ensure orderly evacuation of people and securing human life.
 - ✓ Damage assessment team – assess the extent of damage and also the time period required for recovery at affected site. The team also look into causes of disaster, their impact on extent of damage and expected recovery period.
-

ORGANIZATION AND ASSIGNMENT OF RESPONSIBILITIES

- ✓ Emergency management team – Responsible for overall co-ordination of all the recovery teams. The team is responsible for all activities from activation of the plan to restoration of full operations at original site.
 - ✓ Offsite storage team – responsible for retrieving, packing and shipping of media to the recovery site and also for off site storage of data created at the recovery site.
 - ✓ Software team – Responsible for all OS related activities
 - ✓ Application team – Responsible for all activities relating to application software
-

ORGANIZATION AND ASSIGNMENT OF RESPONSIBILITIES

- ✓ Security team – Responsible for all security related activities at the recovery site
 - ✓ Emergency operation team – Consists of operators and supervisors responsible for systems operations at the recovery site.
 - ✓ Network recovery team – Responsible for all network related activities including WAN
 - ✓ Communication team – Works in conjunction with Network recovery team to establish user/system network. Also co-ordinates with carriers and gate vendors.
-

ORGANIZATION AND ASSIGNMENT OF RESPONSIBILITIES

- ✓ Transportation team – Responsible for transportation of men and material to the recovery site.
 - ✓ User hardware team – Responsible for delivery and installation of end user equipments at the recovery site.
 - ✓ Data preparation and records team – Responsible for updating application database including hiring of data entry personnel at the recovery site
 - ✓ Administrative support team – Responsible for full administrative support both for IP and the employees working at the recovery site
 - ✓ Supplies team – Responsible for arranging all the required supplies at the recovery site
-

ORGANIZATION AND ASSIGNMENT OF RESPONSIBILITIES

- ✓ Salvage team – Makes a more detailed assessment of damage to determine whether planning should be directed towards reconstruction or relocation, provides information for filing insurance claim etc.,
 - ✓ Relocation team – Co-ordinates for moving back to restored original site or to new location.
-

TELECOMMUNICATION NETWORKS

- Telecommunication networks are key to business success and are susceptible not only to natural factors but also to the following unique factors:
 - ✓ Central switching office disaster
 - ✓ Cable cuts
 - ✓ Communication and software glitches and errors
 - ✓ Security breaches
 - ✓ Human mishaps
 - Local exchanges normally do not take on the responsibility of backup services. Organizations have to therefore make their own arrangements.
-

TELECOMMUNICATION NETWORKS

- Methods of providing telecommunication continuity include:
 - ✓ **Redundancy** – involves providing [extra capacity](#) with the intent to utilize the same in the event of normal capabilities are not available.
 - ✓ **Alternative routing** – It is a method of routing information through [an alternative medium without any change in the route](#). Examples include:
 - o Dial up circuit to leased lines
 - o Cellular phone to land lines
 - o Couriers to electronic transmission
-

TELECOMMUNICATION NETWORKS

- ✓ **Diverse routing** – Here medium is same but route is different. This is achieved through split cables or duplicate cables.
 - ✓ **Long haul network diversity** – Here, a different carrier is used to carry the traffic in the event the original network fails.
 - ✓ **Last mile circuit protection** - Here again, a different local carrier is used to carry the traffic in the event of a local communication disaster.
 - ✓ **Voice recovery** -becomes important where business is dependent on voice communication. Choices available are redundancy, alternate routing etc.,
-

INSURANCE

- Not a substitute for actual disaster recovery but nevertheless quite important as many a times this is the only source for funding recovery expenditures.
 - Types of covers available include:
 - ✓ IS Equipment and facilities – provides coverage against physical damage to equipments and other properties.
 - ✓ Media (Software) reconstruction – Covers damage to IS media whether on premises, off-premises or in-transit equal to actual reproduction costs inclusive of programming costs, backup expenses and physical replacement of media.
-

INSURANCE

- ✓ Extra expenses – Covers extra costs of continuing operations following damage or destruction of IP facility.
 - ✓ Business interruption – Covers loss of profit arising out of destruction of IP facilities
 - ✓ Valuable paper and records – Protects against direct physical loss or damage of valuable paper and records
 - ✓ Errors and omissions – Provides legal liability protection in the event a professional commits an act, error or omission that results in financial loss to the client
-

INSURANCE

- ✓ Fidelity coverage – Covers losses from dishonest or fraudulent acts by employees
 - ✓ Media transportation – Covers potential loss or damage to media in transit subject to the condition that all documents must be filmed or otherwise copied.
-

BUSINESS IMPACT ANALYSIS

- BIA (or risk ranking as it may sometimes be called) is fundamental to any BCP/DRP process.
 - BIA include the following:
 - ✓ Determining the information resources required to support critical business operations. Criticality indicators are:
 - o Process supports lives, or peoples' health and safety
 - o Disruption would cost loss of income or prohibitive costs.
 - o Process is required to meet statutory requirements
-

BUSINESS IMPACT ANALYSIS

Examples of critical operations include:

- o Receiving payments
 - o Production
 - o Paying employees
 - o Dispatch of finished goods
 - ✓ Determining the time period in which business process must be resumed. Factors influencing this are:
 - o Trade off between impact of disruption and cost of recovery. Longer the disruption, higher the impact and lower the recovery cost. The relationship is thus inverse.
-

BUSINESS IMPACT ANALYSIS

- o Window of time for recovery may vary depending upon the time of the year or day and/or day of the week
 - ✓ Determining the ranking based on impact of disruption and the probability of occurrence
 - ✓ User involvement is very essential for success of any BIA as criticality is best known to them.
-

BUSINESS IMPACT ANALYSIS

- In summary, BIA aim to classify business process as under:

Classification	Description
Critical	-Cannot be performed without IP facilities -Tolerance is practically zero -Cost of disruption is very high
Vital	-Can be performed manually for a brief period as the cost of manual operations is prohibitive

BUSINESS IMPACT ANALYSIS

Classification	Description
Sensitive	-Can be performed manually at a tolerable cost for an extended period of time. -Extended manual operations not sustainable in the long run.
Non-critical	-Can remain suspended at a little cost. -Require little or no catching up when restored

RECOVERY STRATEGY/ALTERNATIVES

- Based on results of BIA, recovery strategy is selected for each of the IT platform running an application supporting critical business process.

The appropriate strategy is the one ideally balances the impact of disruption and the cost of recovery for an acceptable window of recovery time.

- For handling disasters impairing the primary IP facility, an alternative off site facility is required. Choices are:
 - ✓ Hot site
 - ✓ Warm site
 - ✓ Cold site
 - ✓ Duplicate information processing facility
 - ✓ Reciprocal agreements
-

HOT, WARM OR COLD SITES

- These are usually third part managed sites and differs in terms of degree of preparedness to restore the disrupted operation.

HOT SITE

- ✓ These are *fully configured* and *ready to operate* in few hours.
 - ✓ Add-ons required are staff, programs, data files and documentation.
 - ✓ *Cost is high* and *availability is for a limited time* period as otherwise vendors' promise of protection to other subscribers will begin to impair.
-

HOT, WARM OR COLD SITES

WARM SITE

- ✓ These are *partially configured*.
 - ✓ *CPU is either not available or is less powerful* than required.
 - ✓ Hence, activation is directly the function of time taken for procurement and installation of CPU.
 - ✓ As CPU is the most expensive unit, warm sites tend to be *less costlier than hot site*.
-

HOT, WARM OR COLD SITES

COLD SITE

- ✓ These *have basic environment for operating an IP facility*.
 - ✓ It *does not offer any components* at site.
 - ✓ Activation may take several weeks.
-

DUPLICATE IP FACILITIES

- These are *dedicated self developed recovery sites* that can backup critical operations. The degree of *preparedness is equal to or better than hot sites*.
 - Following principles must be in place for viability of this approach:
 - ✓ The backup site should not be subject to same natural disasters as the original site.
 - ✓ Compatibility of hardware and software should always be ensured.
 - ✓ Capacity enhancements at original site should be accompanied by corresponding enhancements at the backup site.
 - ✓ Testing of backup sites should be performed at regular intervals.
-

RECIPROCAL AGREEMENTS

- These are *between two or more organizations with similar equipments or applications*. Participants promise to provide time to each other when emergency occurs.
 - ✓ Advantages – Low cost. May be the only option due to unique vendor equipment.
 - ✓ Disadvantages – Usually not enforceable. Creeping differences in hardware including changes in capacity and /or software may render the agreement to be of limited use only.
 - ✓ Critical points in reciprocal agreements:
 - o How much time will be made available?
 - o What facilities and equipments will be available?
-

RECIPROCAL AGREEMENTS

- o Will staff assistance be provided?
 - o How long can the emergency operations continue?
 - o How frequently can the compatibility be tested? How much advance notice is required?
 - o Are there any parts of the year or month etc., when partner facilities are not available.
-

CONTRACTS WITH HOT, WARM OR COLD SITE VENDORS

- Contractual provisions for the use of third party sites should cover:
 - ✓ Vendor's configurations vis-a-vis changing needs of the company
 - ✓ Definition of the disaster
 - ✓ Speed of availability
 - ✓ Subscribers per site
 - ✓ Subscribers per area
 - ✓ Preference if there are common or regional disaster
 - ✓ Insurance for company employees at vendor site
-

CONTRACTS WITH HOT, WARM OR COLD SITE VENDORS

- ✓ Usage period
 - ✓ Vendor's warranties
 - ✓ Right to audit
 - ✓ Right to test
 - ✓ Reliability
-

BACKUP HARDWARE PROCUREMENT

- Procurement of backup hardware becomes important when recovery strategy is based on warm/cold site or recovery period is prolonged requiring movement from hot to warm or cold site.
 - Possible sources are:
 - ✓ Original vendor
 - ✓ Used hardware market
 - To facilitate backup hardware procurement, the following strategy may be considered for adoption:
 - ✓ Avoid using unusual or hard to get equipment
 - ✓ Updating equipment to keep current
 - ✓ Maintaining software compatibility to permit operation of new equipments
-

MEDIA AND DOCUMENTATION BACKUP

- Periodic backup of data and the connected software is absolutely essential for success of any BCP/DRP.
 - Back schedules may vary depending upon the application. Generally the following factors should be considered in determining the frequency of backup cycle and depth of retentions:
 - ✓ Failure could happen at any stage of processing cycle.
 - ✓ In batch mode processing,
 - o Master files should be retained at appropriate intervals such as at the end of updating procedure.
 - o Transaction files should be presented to coincide with the master files
-

MEDIA AND DOCUMENTATION BACKUP

- ✓ Real time files may require special techniques such as
 - o Duplicate logging of transactions
 - o Before and after image of master records
 - o Time stamping of transactions
 - ✓ DBMS may require specialized backup including data dictionaries.
 - Backup must include object code and source code libraries,
 - Software license if required for operations at alternative site should be arranged in advance.
 - Automation of backup procedure should be considered where required.
 - A set of backups must always be kept at off-site and given the same level of security as the original.
-

OFF SITE STORAGE

- Off site storage is critical to recovery when primary site is destroyed partially or fully.
 - Apart from MEDIA AND DOCUMENTATION, off site storage may include:
 - ✓ Operating procedures
 - ✓ System program and documentation
 - ✓ Special procedures
 - ✓ Input source documents
 - ✓ Output documents
 - ✓ Business continuity plan
 - An inventory of contents at off site should be maintained.
-

OFF SITE STORAGE

- Controls over off site storage should be at par with those at the original site.



SECURITY AND CONTROL OF OFFSITE FACILITIES

- Should be secured and controlled as the original site.
- Should not be easily identifiable to prevent intentional sabotage of offsite should the destruction of original site be from a malicious attack



RECOVERY/CONTINUITY PLAN TESTING

- Testing is a must to determine the effectiveness of the proposed measures in handling a disaster when it occurs.
 - The test should be so scheduled as to minimize disruptions to normal operations. Weekend are generally a good time.
 - Key recovery team members must be fully involved.
 - Actual prime time conditions should be simulated even if test is done in off hours.
 - **Specifications** – Test should try to accomplish the following:
 - ✓ Verify completeness and precision
 - ✓ Evaluate performance of persons involved
 - ✓ Appraise the training and awareness level of non BCP team members
-

RECOVERY/CONTINUITY PLAN TESTING

- ✓ Evaluate level of coordination among BCP team and external agencies
 - ✓ Measure the ability and capacity of backup site to perform
 - ✓ Assess vital records retrieval capability
 - ✓ Evaluate the state and quantity of equipments and supplies actually relocated to backup site.
 - ✓ Measure the overall performance in terms maintaining critical business process
-

RECOVERY/CONTINUITY PLAN TESTING

- **Test types** – The following type of tests may be performed
 - ✓ Paper test – A structured walk through of the plan
 - ✓ Preparedness test – Test is performed on different aspects of the plan by simulating a portion at a time. This a cost effective way of obtaining evidence on how good the plan is.
 - ✓ Full operational test – Test is performed simulating the disaster in full short of actual disruption of service. For testing purposes, this is the disaster.
-

RECOVERY/CONTINUITY PLAN TESTING

- **Test phases** – Test is performed in following phases:
 - ✓ Pre-test – Actions necessary to set the stage for actual testing
 - ✓ Test – Actual operation activities are executed and evaluators review staff members as they perform designated tasks.
 - ✓ Post-test – Cleaning up of the area. Formal evaluation of the plan and implementation of improvements.
 - **Documentation of results** – During every phase, detailed documentation should be maintained to facilitate analysis of strengths and weaknesses of the plan
-

RECOVERY/CONTINUITY PLAN TESTING

- **Results analysis** – Results must be quantitatively gauged using following measures:
 - ✓ Elapsed time
 - ✓ Amount of work performed
 - ✓ Number of records recovered versus required, number of supplies/equipments requested versus actually received etc.,
Number of critical systems successfully recovered
 - ✓ Accuracy at backup site versus normal accuracy
-

RECOVERY/CONTINUITY PLAN MAINTENANCE

- BCP/DRP should be reviewed and updated at periodical intervals to reflect the changing environment. Factors contributing to changes are:
 - ✓ Changes in business strategy leading to changed criticality of the business processes.
 - ✓ Changes in software or hardware environment
 - ✓ Development of new applications
 - ✓ Availability of new recovery alternatives
 - Maintenance responsibilities include:
 - ✓ Developing schedule for review/maintenance
 - ✓ Review of revisions, comments and suggestions
-

RECOVERY/CONTINUITY PLAN MAINTENANCE

- ✓ Arranging and participating in testing of the plan
 - ✓ Training of recovery personnel
 - ✓ Updating notification directory
 - ✓ Record of maintenance activities
-

AUDIT OF BCP/DRP

- Is auditor tasks include:
 - ✓ Review of BCP
 - ✓ Evaluate prior test results
 - ✓ Evaluate offsite storage
 - ✓ Interview key personnel
 - ✓ Evaluate security at offsite facility
 - ✓ Review contracts for alternate IP facilities
 - ✓ Review insurance coverage
-

Questions

1. During an audit of a reciprocal disaster recovery agreement between two companies, the IS auditor would be PRIMARILY concerned about:
 - A. the soundness of the impact analysis.
 - B. hardware and software compatibility.
 - C. differences in IS policies and procedures.
 - D. frequency of system testing.
-

Questions

2. An IS auditor has observed the test of a disaster recovery plan. Following the test, the IS Auditor would NOT be expected to:
- A. review results of telecommunications tests at remote sites.
 - B. ensure the tests results met all business objectives.
 - C. update the disaster recovery plan.
 - D. document recommendations for changes to the plan.
-

Questions

3. An IS Auditor reviewing the results of a test of the disaster recovery plan conducted at a warm site notes that clients were unable to log-on to the restored on-line systems as there were insufficient data lines connecting the client premises to the recovery site. The MOST likely conclusion that the IS auditor would draw is that the:
- A. clients were not sufficiently involved in plan development
 - B. use of a warm site is inappropriate
 - C. impact of a potential disaster was not fully analyzed
 - D. external communications service providers were not involved in the test
-

Questions

4. Which of the following methods would **BEST** ensure the adequacy of the disaster recovery plan?
- A. Regular reviews of the currency of the information detailed in the plan
 - B. Unannounced shut down of the primary installation during quiet periods
 - C. Regular recovery exercises using expert personnel, trained in the execution of the recovery procedures
 - D. Unannounced recovery exercises at regular intervals
-

Questions

5. Which of the following is a risk if system backups are only performed weekly?
- A. System defaults are inaccurate
 - B. System files are not synchronized with data access
 - C. System files are partially fragmented
 - D. System defaults are lost
-

Questions

6. An IS Auditor discovers that an information processing facility's business continuity plan provides for an alternate processing site which will accommodate fifty percent of the primary processing facility's processing capability. Based on this discovery, which of the following actions should the IS auditor take?
- A. Do nothing, because generally, less than twenty-five percent of all processing is critical to an organization's survival and the backup capacity is therefore adequate.
 - B. Identify applications that could be processed at the alternate site and develop manual procedures to back up other processing.
 - C. Ensure that critical applications have been identified and that the alternate site could process all such applications.
 - D. Recommend that the information processing facility arrange for an alternate processing site with the capacity to handle at least seventy-five percent of normal processing.
-

Questions

7. An IS Auditor should be involved in:

- A. observing tests of the disaster recovery plan
 - B. developing the disaster recovery plan
 - C. maintaining the disaster recovery plan
 - D. reviewing the disaster recovery requirements of supplier contracts.
-

Questions

8. Which of the following is the LEAST probable consequence of poor disaster recovery procedures?
- A. Company revenues may be lost
 - B. Organizational productivity may be disrupted
 - C. Critical data may be lost
 - D. The company may go out of business
-

Questions

9. When implementing an application software package, which of the following presents the greatest risk?
- A. Multiple software versions not controlled
 - B. Source program not synchronized with object code
 - C. Parameters not set correctly
 - D. Programming errors
-

Questions

10. The window of time for recovery of information processing capabilities is based on the:
- A. Criticality of the operations affected
 - B. Quality of the data to be processed
 - C. Nature of the disaster
 - D. Applications that are mainframe based
-