Business continuity planning

<u>Case Study:</u> Swift Pipes Limited manufactures various types of pipes used in construction industry. During last monsoon season, its data center was badly impacted by heavy rain causing unavailability of IT system that lead to suspension of operations for a week. Since the position of IT Manager is lying vacant, the management asked Ahmed, an employee of the IT department to develop a Disaster Recovery Plan (DRP) for IT operations. Ahmed downloaded DRP of a reputed company engaged in similar business from internet and after making nominal changes, presented it to the management for approval.
On interviewing Ahmed, the CFO was quite irritated with the approach. He rejected the DRP altogether and asked a senior member of his department to carry out the task again.

One of the key **<u>drawbacks in the approach adopted by Ahmed</u>** was that he did not consider any internationally accepted standard or guideline for developing the DRP.
Moreover, he considered the nature of business only and seemed to have ignored other factors altogether. For example, differences between the two companies may exist on the following accounts:
 available resources
 dependence on IT systems
 recovery point objective
 recovery time objective etc.
 size of organisation
 risks specific to SPL and the risks related to the organisation whose DRP was copied

A DRP comprises of the following **four types of plans:**

Emergency Plan: It specifies actions to be undertaken immediately when a disaster occurs, including the situations when the plan is to be invoked, who is to be notified, actions to be undertaken, evacuation procedures and return procedures.

Backup Plan: It specifies type of backup, frequency of backup, procedures, location of resources, backup site, personnel, priorities/sequence and time frame for recovery.

Recovery Plan: It varies on the type and scale of disaster, and sets out procedures for quick restoration of information systems and operations. It usually identifies a recovery committee to decide on measures, and specifies responsibilities of individuals and guidelines on priorities.

Test Plan: It enables the DRP to be tested so that deficiencies in all the plans or in the preparedness of the organization and its personnel are identified and fixed in a timely manner. This plan must be invoked periodically with simulated disasters and ensure improvements are made.

<u>DRP VS BCP:</u> A DRP is designed to restore operability of the target systems, applications or computer facility at an alternate site after an emergency. A BCP enables a company to respond to an interruption in such a manner that critical business functions continue with planned level of interruption or essential change. Usually, DRP is a part of BCP. SPL should also develop a BCP if it wants to minimize the loss due to interruption.

<u>Phases of Business Continuity Planning Process and activities performed in each phase.</u>

Phase 1: Initiating the BCP Project
• Obtain and confirm support from senior management.
• Identify key business and technical stakeholders.
• Form a business continuity working group.
• Define objectives and constraints.
• Establish strategic milestones and draw up a road map.
• Begin a draft version of business continuity policy.
Phase 2: Assessing Business Risk
• Conduct risk analysis workshops.
• Assess the likelihood and impact of threat occurrence.
• Categorize and prioritize threats according to risk level.
• Discuss outputs of risk analysis with management.

- Ascertain level of risk acceptable to the organization.
- Document outputs in business continuity policy.

Phase 3: Preparing for Possible Emergency

- Identify critical and noncritical business services.
- Establish preferred business continuity service levels and profiles for continuity and recovery.
- List the potential emergencies that include events that occur within the facility and/ or outside the facility.
- Estimate the probability of occurring such emergency.
- Prepare a backup plan.
- Identify backup facilities/site types to be arranged i.e. hot site, cold site etc.

Phase 4: Disaster Recovery Phase

- Assess the potential of human impact (possibility of death or injury).
- Assess the potential property impact (loss of property, machines, etc.)
- Assess the business impact (business interruption, critical supplies interruption, etc.)
- Identify teams and assign responsibilities during disaster recovery phase.
- Prepare contact list of key personnel.
- Assess readiness based on internal and external resources.

Phase 5: Business Recovery Phase

- Identify and engage potential business continuity partners.
- Draft a detailed set of continuity plans and work toward an agreed set of plans with senior management.
- Produce and execute an implementation plan.

Phase 6: Testing the Business Recovery Process

- Define business continuity acceptance criteria.
- Formulate the business continuity test plan.
- Identify major testing milestones.
- Devise the testing schedule.
- Execute tests via simulation and rehearsal; document test results.
- Assess overall effectiveness of business continuity plan; pinpoint areas of weakness and improvement.
- Iterate tests until the plan meets acceptance criteria.
- Check, complete, and distribute business continuity policy.

Important steps in **evaluating the effectiveness and comprehensiveness of a BCP** are as follows:

- Obtain a copy of the updated Business Continuity Plan.
- Sample the distributed copies of the plan and verify that they are current.
- Evaluate the procedure for updating the manual. Are updates applied and distributed in a timely manner? Are specific responsibilities for maintenance of the manual documented?
- Determine if all applications have been identified and reviewed for their level of tolerance in the event of a disaster.
- Evaluate the effectiveness of the documented procedures for the initiation of the business continuity effort.
- Review the identification and planned support of critical applications, including PC based or end user developed systems.
- Determine if the alternative processing site has the correct version of the software.
- Determine if the alternative processing site does not have the same environmental risks as faced by the original site.
- Review the list of business continuity personnel, emergency hot site contacts, emergency vendor contacts, etc. for appropriateness and completeness.
- Actually call a sample of concerned personnel and verify that their phone numbers and addresses are correct as indicated. Interview them for an understanding of their assigned responsibilities in a disaster situation.
- Determine if all recovery teams have written procedures to follow in the event of a disaster.
- Determine if items necessary for the reconstruction of the information processing facility are stored off-site, such as blueprints, hardware inventory and writing diagrams.
- Check if the critical information assets are protected under insurance cover.
- Determine if the BCP has ever been tested or is there any mandatory requirement to test the BCP at periodic intervals?

The following **factors** should be considered while devising future **recovery strategy**:

Recovery Point Objective (RPO): It indicates the pre-incident point in time that data must be recovered. For example, if an organisation may afford to lose data up to two hours before disaster, then the latest data backup available should be at least two hours before the interruption or disaster.

Recovery Time Objective (RTO): It indicates the earliest point in time at which the business must resume after disaster. It is based on the acceptable downtime in case of a disruption of operations.
Interruption Window: It is the time organization can wait from the point of failure to the critical services/applications restoration. After this time, the progressive losses caused by the interruption are unaffordable.
Service Delivery Objective (SDO): It is the level of services to be reached during the alternate process mode until the normal situation is restored.
Maximum Tolerable Outages: It is the maximum time the organization can support processing in alternate mode. After this point, different problems may arise, especially if the alternate SDO is lower than the usual SDO and the information pending to be updated can become unmanageable.

Based on the above factors, an organisation decides how much resources it has to deploy to achieve Business Continuity. For example if RPO is in minutes then data mirroring or duplexing should be implemented as the recovery strategies. If the RTO is lower, then the alternate site might be preferred over a hot site contract.

Though FS had a comprehensive Business Continuity Plan (BCP) in place, some of its IT systems may have failed for extended periods on account of the following reasons:

- BCP was not updated.
- BCP was not comprehensively tested.
- FS had not trained its employees to cope up with disastrous situations and make use of BCP.

Key differences between hot, warm and cold sites are as follows:

Hot site	Warm site	Cold site
It is a fully operational offsite data processing facility equipped with both hardware and system software compatible with the primary installation being backed up.	It is partially configured, usually with network connections and disk drives but without the main computer or with a less powerful CPU.	It does not have computer equipment in place, however, it is ready to receive such equipment.

Responsibilities of the person accountable for the maintenance of BCP are as follows:

- Development of a schedule for periodic review and maintenance of the plan.
- Advising all personnel of their roles, inviting any revisions and comments within a certain period.
- Review of revisions and comments and updating the plan within a specified period, say 30 days, of the review date.
- Arranging and coordinating scheduled and unscheduled tests of the business continuity plan to evaluate its adequacy.
- Participating in the scheduled plan tests performed at least once per year on specific dates.
- For scheduled and unscheduled test, writing evaluations and integrate test results into the business continuity plan within a specified period, say 30 days. / Documenting the test results and integrating these into the BCP.
- Training recovery personnel in emergency and recovery procedures as set forth in the BCP.
- Updating notification directory of all personnel including phone numbers, responsibilities or status within the company, etc.
- Calling for unscheduled revisions whenever significant changes occur.
- Maintaining records of business continuity plan maintenance activities, i.e. testing, training and reviews.

.

Responsibilities of new appointee relating to maintenance of BCP:

- Developing a schedule for periodic review, testing and maintenance of the plan.
- Advising all personnel of their roles and the deadlines for receiving revisions and comments.
- Calling for unscheduled revisions whenever significant changes occur.
- Arranging and coordinating scheduled and unscheduled tests of the BCP.
- Training of personnel for emergency and recovery procedures.
- Maintaining records of business continuity plan maintenance activities, i.e. testing, training and reviews.
- Evaluate and integrate changes to resolve unsuccessful test results into the BCP.

- Administer the change management process for the changes identified other than BCP testing activity. (*The change management process includes: identification of changes, acquiring approval for identified changes and incorporating/documenting the changes after approval*)

Importance of an updated Business Continuity Plan

- A BCP which is not updated may fail to safeguard the company from disruption, in case of a disaster.
- There may be missing links in the recovery procedures and consequently the procedures may fail or the recovery may be delayed significantly.

BCP should be **reviewed and updated**, if needed, when:

- a new application is developed/acquired and implemented.
- a business strategy is changed or updated.
- software or hardware environment is changed.
- at regular predetermined intervals even if none of the above occurs.

Circumstances which create the need for **BCP updation:**

- Changes in business strategy may alter the significance of various applications.
- Acquisition/development of new resources/applications.
- Changes in software or hardware environment may make current provisions obsolete or inappropriate or inadequate.
- Change in roles and/or responsibilities of Disaster Recovery plan/ Business Continuity Plan (DRP/BCP) team members.
- Change in arrangement with the vendors.
- Material weaknesses found during testing of BCP.
- A change in the needs of the organization.
- Change in regulatory requirements.

Case study: Swift Tyres Limited (STL) is developing a recovery strategy for its information processing systems. The IT head has identified the following types of recovery sites to the board of directors:

1. Duplicate information processing facilities.
2. Offsite backup hardware facilities including hot, warm and cold sites.
3. Reciprocal arrangement with other companies.

After due deliberation, the board has shown its inclination towards the option of reciprocal arrangement. The chairman, however, commented that such an arrangement is more challenging than other proposed options and added that if not properly worked out, a reciprocal arrangement could enhance the damages.

Reciprocal arrangements are between two or more organisations with similar equipment or applications. The participants commit to provide computer time to each other when an emergency arises.

The board might have considered the fact that since STL is a manufacturing concern its information systems have higher **tolerance** to interruption than the organisations such as banks. Hence it may not need to go for duplicate information processing facility or hot site which are much expensive options and are designed for very low tolerance systems. Moreover, if due care is taken in selecting the reciprocal party and drafting the agreement, such arrangement may take less time to become functional as compared to warm /cold site.

The chairman might have felt reciprocal arrangement more challenging than other options because of the following reasons:

- It is difficult to find another organisation with 100% similar equipment and assurance of availability when needed.
- Assurance of availability often necessitates significant compromises on differences in equipment configuration which in turn results in ineffective operations.
- Un-notified changes in workloads, equipment configurations or any unforeseen dispute between the parties may render the agreement limited or useless.
- Confidentiality requires special consideration. This is because the damaged organisation is placed in a vulnerable position while needing to trust the sponsoring party housing the victim's confidential information.

STL should consider following matters while entering into an agreement of reciprocal arrangement:
(i) Clear identification of available facilities and equipment.
(ii) Minimum/maximum lead time to gain access to the host recovery site. / Requirement of any advance notice for using the facility.
(iii) Extent of staff assistance provided, if any.
(iv) Maximum time span for running operations from recovery site.
(v) The type of security that would be implemented to safeguard information systems operations and data.
(vi) Frequency with which systems could be tested for compatibility.

Case study: Prestige Communications (PC) and Natural Technologies (NT) have recently entered into a reciprocal agreement which will allow each party to use the processing facilities available with the other, in case of disaster. PC has requested their IT Manager to review the reciprocal agreement to ensure that it covers all critical areas.

Questionnaire for the IT Manager to help him ensure that the agreement is complete in all aspects.

- ✓ What facilities, equipment and software will be available?
- ✓ Will staff assistance be provided?
- ✓ How quickly can access be gained to the host recovery facility?
- ✓ How long can the emergency operation continue?
- ✓ How frequently can the system be tested for compatibility?
- ✓ How will confidentiality of the data be maintained?
- ✓ What type of security will be afforded for information systems operations and data?
- ✓ Are there certain times of the year, month, etc. when the partner's facilities shall not be available?
- ✓ Whether costs to be billed have been agreed upon clearly?
- ✓ Has appropriate clauses been included to ensure that commitment is fulfilled? (e.g. penalty clause)
- ✓ Does the agreement contain appropriate provision as regards the termination of the contract?

Case study: TN Limited (TNL) had so far been using simple back-up procedures to safeguard its data. It has now developed a comprehensive Business Continuity Plan (BCP) under which arrangements have been made with a third party for using their processing facilities. Under the proposed agreement, the third party would provide the necessary hardware on which TNL's software will remain installed, for its use, in case of a disaster.

Following issues must be covered clearly in the agreement:
- How soon the site will be made available subsequent to a disaster?
- The period during which the site can be used.
- The conditions under which the site can be used.
- The facilities and service the site provider agrees to make available.
- What controls will be in place and working at the alternative facility.
- The priority to be given to concurrent users of the site in the event of a common disaster.
- Frequency with which the system could be tested / audited for compatibility.
- Payment terms should be clearly explained.
- Inclusion of penalty clause to ensure fulfillment of commitment.
- Appropriate provision as regards the termination of the contract.

BSL should consider the following **key factors** before entering into hot site agreement with SL:
(i) Configuration: are the SL's hardware and software configurations adequate to meet BSL needs?
(ii)Disaster: Is the definition of disaster agreed by SL broad enough to meet anticipated needs of BSL?
(iii)**Environmental/Social/Political Risk:** If BSL and SL are at significantly different locations, they may have different level and nature of environmental/social/political risks.
(iv)Speed of Availability: How soon after the disaster, will facilities be available to BSL? How much advance notice is required for using the facility?
(v)Number of Subscribers: Does SL define any limit to the number of subscribers at the facility offered to BSL?
(vi)Preference: Does SL agree to give BSL preference if there is a common or regional disaster? Is there any backup of the hot site offered by SL? Does the SL have more than one facility available for its clients?

(vii)Insurance: Is there adequate insurance coverage for BSL's employees at the SL's site? Will existing insurance company of BSL reimburse those fees?
(viii)Usage Period: For how long SL's facility would remain available for use? Would it remain available for an adequate time? Are there certain times of the year, month etc when SL's facilities are not available?
(ix)Technical Support: What kind of technical support will SL provide? Does it seem adequate?
(x)Communications: Are the communication connections to the SL's site sufficient to permit unlimited communication with it, if needed?
(xi)Warranties: The type of warranties that would be provided by SL regarding availability of the site and the adequacy of facilities?
(xii)Confidentiality Measures / Controls: Are there adequate controls implemented by SL to ensure confidentiality of BSL's data?
(xiii)Audit: Is there a right-to-audit clause in the contract, permitting an audit of the site to evaluate logical, physical and environmental security?
(xiv)Testing: IS SL ready to allow periodic testing of its facility and equipment?

Case study: Sohrab Insurance Company (SIC) specialises in health insurance. In December 2014, fire broke out in SIC's data processing facility which forced SIC to operate from a hot site facility. However, SIC faced lot of difficulty in getting access to the site and completing data processing tasks. A consultant hired by SIC has reported that most of the difficulties arose because of deficiencies in the agreement with the hot site provider.

Probable deficiencies in the agreement are briefly discussed below:

Configurations: Required configuration of hardware had not been specified and vendor's hardware and software configurations might have been found to be inadequate to meet company needs.
Disaster: The definition of disaster may not be broad enough to meet the anticipated needs. Hence, the vendor might have taken time in agreeing to treat the incidence as disaster and handing over the facility to SIC.
Speed of availability: The time within which the site would be made available may not have been specified or
longer than required time may have been specified.
Preference: In case of shared hot site the agreement may not be cleared as to arrangements if more than one client requires the use of the hot site.
Communications: The agreement may be silent over minimum acceptable communication facilities and hence the communication facilities provided by the vendor might be inadequate.
Warranties / Penalty clauses: The agreement may be silent over warranty regarding availability of the site and the adequacy of the facilities. Thus the vendor might not have provided adequate facilities and/or access to the site on time as for non-fulfillment of commitment; he is not subject to any penalty.

Critical Recovery Time Period (CRTP):

It is the time in which business processing must be resumed before suffering significant or unrecoverable losses. The length of this time period always depends on the nature of the business being disrupted. CRTP also depends on the time of disruption i.e., month, week, day, time etc.

Ranking of Business in terms of CRTP:

Generally, banks have the shortest CRTP because online banking transactions (involving internal as well as external stakeholders) are now carried out round the clock and any disruption at any stage proves costly in terms of financial loss as well as loss of reputation.

As regards the CRTP of a manufacturing company and an insurance company, the duration of the CRTP would depend upon their degree of reliance on IT. For example, those manufacturing companies whose entire operations including manufacturing are IT based would have a shorter CRTP. Similarly, if the number of daily transactions is high in the case of an insurance company, as is the situation involving life and marine insurance, the CRTP would be shorter. Comparatively, those insurance companies which deal only in motor, fire and other such types of insurances, the CRTP would be much longer.

System Risk Ranking: This involves determination of **risk** based upon the impact derived from the critical recovery time period, as well as the **likelihood** that an adverse disruption will occur.

A typical risk ranking system may contain the following classification:

(i) Critical: These functions cannot be performed unless they are replaced by identical capabilities. Critical applications cannot be replaced by manual methods. Tolerance to interruption is very low as costs of interruption are very high.

(ii) Vital: These functions can be performed manually but for a brief period of time. There is higher tolerance to interruption than with critical systems and therefore, somewhat lower costs of interruption provided that functions are restored within a certain time frame (usually within 5 days).

(iii) Sensitive: These functions can be performed manually, at tolerable cost, for an extended period of time. While they can be performed manually, it is usually a difficult process and requires additional staff to perform and also results in inefficiencies.

(iv) Non-critical: These functions may be interrupted for an extended period of time, at little or no cost and require little or no efforts to update the system after restoration.

A detail and **updated inventory list** is important in quick restoration of the systems as it:

- helps to quickly identify the exact details of the asset that need to be replaced;
- curtails the search time to find the replacement asset immediately as it identifies the location of any similar/redundant asset;
- expedites getting the approval process for movement of the replacement asset as it identifies the owner of the asset who can be contacted for urgent change in custodianship; and
- helps to make quick risk assessment before moving an asset.

Data classification helps quick restoration of the systems as it:

- identifies the access rights of individuals which help in selection of people for retrieving data from backups and other related systems;
- identifies the persons who can be contacted for allowing access rights at various levels; and
- helps to implement desired level of security on the restored system.

Correct **system risk ranking** is useful in quick restoration of the systems as it identifies the systems:

- restoration order i.e., in which the systems should be restored.
- whose prolong unavailability can be sustained.
- that need exact capabilities to be restored.
- whose functions can be performed manually for a brief period of time.
- whose functions can be performed manually for an extended period of time.

The **risk management process** involves the identification and classification of **assets**, assessing the **threats** associated with the identified assets, identifying vulnerabilities or lack of controls and assessing the **impact** of the identified threats.

Assets relating to IT	Threats	Impact	Controls
Information/data	□ Errors	• Business interruption • Monetary loss	• Users' training • Input and verification by different persons • Data validation checks.
	□ Malicious damage/attack □ Viruses □ Hackers	• Denial of service • Business interruption • Loss of business opportunity • Loss of data • Monetary loss	• Properly configured firewall • Installing updated definitions of anti-virus programs • Restricting use of removable drives. • Proper backup plan

	□ Theft	• Loss of business opportunity • Leakage of business secrets. • Legal repercussions	• Use of strong passwords • Use protected communication lines for data transmission • Restricting use of removable drives.
	□ Electric Surge	• Loss of data • Business interruption.	• Proper maintenance of water fittings • Using stabilizers and circuit breakers • Proper maintenance of electric circuitry
Hardware	□ Theft	• Business interruption • Monetary loss	• Security guards • Lock and key • Digital locks • Biometric locks • Prohibiting one person to work alone.
	□ Equipment failure □ Physical damage	• Business interruption • Loss of business opportunity	• Hardware backup • Periodic maintenance • Maintenance contracts
	□ Electric Surge	• Loss of equipment • Business interruption.	• Proper maintenance of electric fittings • Using stabilizers and circuit breakers
	□ Fire	• Business interruption • Loss of equipment and facilities.	• Fire proof rooms • Alternative hardware and facilities arrangement • Fire alarms • Fire extinguishers.
	□ Water	□ Business interruption □ Loss of data.	□ Proper maintenance of water fittings and drainage system □ Raised floors
Software	□ Program errors □ Bugs □ Trap doors	• Business interruption • loss of data • loss of confidentiality	• Testing before implementation • Source code review • Software maintenance
	□ Malicious damage/attack	• Denial of service • Business interruption • Loss of business opportunity • Loss of data	• Properly configured firewall • Installing updated definitions of anti-virus programs • Restricting use of removable drives.
	□ Use of pirated software	• Legal consequences • Loss of reputation	•Compliance of software licenses • Prohibiting users from installing programs
Personnel	□ Health hazards	• Business interruption	• Proper work environment • Proper job description • Mandatory vacations.
	□ Injuries	• Business interruption	• Proper maintenance of electric fittings

			• Wet floor cautions.
	□ Resignation	• Business interruption	• Succession planning • Program documentation.
	□ Death	• Business interruption	• Succession planning • Program documentation.

<u>Case study:</u> The office of Future Limited (FL) had replaced all its firefighting equipment in 2007 with a state of the art fire detecting system. The management claims that the system can detect even a minor flame. As soon as a fire is detected, the extinguisher system is activated and a gas suppressant is dumped into the particular area after 60-seconds. Staff members have been instructed to evacuate the office immediately when the alarm is triggered because the suppressant is somewhat toxic.

<u>Comments</u>: Future Limited (FL) has placed complete reliance upon the fire suppressant system. It is not clear whether FL has given any fire-fighting training to its staff and whether the system has been regularly tested and serviced. Further it seems that if the alarm system fails in the event of fire or if the staff members are unable to evacuate from the facility within 60 seconds, their lives may be endangered. FL should, therefore, employ additional firefighting tools such as hand-held fire extinguishers, fire blanket, oxygen mask and manual activation of alarm etc., to strengthen its fire-fighting capacity.

To carry out a full scale **review** of the adequacy of the fire-fighting capabilities at FL's premises, I would:

- ➢ determine if there exist alternate procedures for firefighting if the fire detection system fails to operate.
- ➢ determine if a fire occurs at a point within the server room or anywhere in the office, will the staff be able to safely vacate from the premises before the toxic suppressant is dumped.
- ➢ check if there exists any emergency exit in case of fire.
- ➢ ensure that the sound (of alarm) produced by the system is so peculiar so as to be clearly distinguishable.
- ➢ check any documentary evidence if the fire detection system is regularly tested and serviced.
- ➢ check any written records of any fire incident that may have occurred in the past to evaluate how the procedures were applied.
- ➢ interview individuals to examine their understanding of the fire detection system and evacuation procedures.

The **objectives for a typical test plan** of a **BCP** are as follows:

- ❖ To verify the completeness and precision of the BCP.
- ❖ To evaluate the performance of the personnel involved in the BCP.
- ❖ To appraise the training and awareness of the teams.
- ❖ To evaluate coordination between BCP teams, DRP teams, external vendors and service providers.
- ❖ To measure the ability and capacity of the backup site to meet the organisation's requirements.
- ❖ To assess capability to retrieve vital records.
- ❖ To evaluate the state and quantity of equipment that have been relocated to the recovery site.
- ❖ To measure the overall performance of the operational and processing activity of the organisation.

Following **steps** should be taken **after test of a BCP** has been carried out:

- Returning all resources to their proper place.
- Disconnecting equipment and returning personnel.
- Deleting all company data from third-party systems.
- Documentation of observations, problems and resolution.
- Communicating results to the management.
- Formally evaluating the plan.
- Implementing indicated improvements.

Paper Walk-through Test:
In this type of test major players in the plan's execution reason out what might happen in a particular type of service disruption. They may walk through the entire plan or just a portion.

Preparedness Test:
These tests are usually performed in respect of smaller components of the IT System i.e. in respect of one or two areas of operation only. These are usually performed at the entity's own processing facility and prepare it for a full operational test at a later stage.

Full Operational Test:
This is the full scale testing in which users pass through the simulation of system crash as it happens in real. All IT operations at the original site are shut down and the processing facilities are recovered at the backup/alternative recovery site. This test requires all players of the team to participate actively and play their roles as described in the BCP.

Case study: You have recently joined as IT Manager of Smart Finance Securities (SFS) which is a reputable medium-sized share brokerage house. SFS processes an average of 10,000 transactions in a day.

Though SFS can retrieve record of transactions of the preceding 30 days from the stock exchange, full back up is also recorded on magnetic tapes on every alternate day. Such backup is maintained for three months.

Former IT Manager had proposed to replace the existing backup method with a real time back-up mirrored on the live (same) server. He had also proposed to record monthly backups on DVDs which would be retained for 12 months.

However, the CEO had opposed the idea because he was of the view that SFS should simply retrieve monthly backups of its transactional data from the stock exchange and retain it for one year. According to the CEO even the current backup procedures are not necessary.

Comments on current backup strategy: SF's current backup strategy is useful in conjunction with retrieving record from stock_exchange. However, recording full back up on every alternate day leads to handling of 36 tapes in three months which seems inefficient and cumbersome. A better approach is stated in recommendation.

Comments on strategy proposed by former IT Manager: One of the key objectives of adopting real-time backups or mirroring strategy is to establish a 'failover' mechanism. If the backup is taken on the same machine, it would defeat the purpose of failover because if the server crashes, the backup will not be available to facilitate the failover requirement, and the backups may also be lost.

The effectiveness of monthly backup will diminish with each passing day of the following month. It is only useful in conjunction with the backup retrieved from the local stock exchange.

Comments on CEO's view: CEO's idea of retaining one year backup is good as it would enhance the company's ability to retrieve 12 months data as compared to present policy of maintaining 3 months backup. However, discontinuation of recording own backup set would create strong dependency on local stock exchange.

Recommended policy and justification: SF may have three sets of backups, i.e., daily, weekly and monthly. The daily backup tapes_are re-used (recycled) in the following week, and the weekly backup tapes are re-used in the following month while the re-usability of monthly backup tapes depends upon the backup retention period. For example, if only three months backup is to be retained then the monthly backup can be re-used after every three months. Similarly, if backup is to be retained for a year, it should not be re-used before 12 months. At year-end, full year backup may be taken which could be retained on a permanent basis for reference and risk avoidance.

For a three months backup, the above policy would require only 12 tapes as follows:

□ 5 tapes for daily backup;
□ 4 tapes for weekly backups; and
□ 3 tapes for monthly backups.

This shows that three times less tapes would be used as compared to the current backup strategy.

The daily backups are recorded on week days, in which at least one full backup is created each week; the rest of that week's backups can be differential. Weekly and monthly backups should always be taken as full backups of the week and month respectively. Taking real-time backup on another server at another location would provide further security against loss of data during a particular day.

Besides taking backup, the SFS should take the following steps to ensure that it is able to restore the data whenever required:

- Specific duties should be assigned for recording and restoration of backup.
- Physical Backup tapes should be checked periodically to ensure that all tapes are available for completed years, months, weeks and days.
- Any change in backup plan or in duties of the responsible persons or in the location of the backup storage should be properly documented.
- The backups should be restored periodically to ensure that system could be restored from the available backups.
- Backups should be stored at a suitable distance from the main IT site so that they may be available when required for disaster recovery. Preferably, backup storage location shall not be subject to the same social and environmental threats as that of the original site.
- Necessary training should be provided to the staff responsible for recording and restoration of data.

Following types of **risks**, related to information systems processing facilities, may be **insured:** (P-317)

- IS Facilities – provides coverage about physical damage to the information processing facilities.
- IS Equipment – provides coverage about physical damage to the owned equipment.
- Media (software) reconstruction – covers damage to IS media that is the property of the insured and for which the insured may be liable.
- Extra expense – designed to cover the extra costs of continuing operations following damage or destruction at the information processing facility.
- Business interruption – covers the loss of profit due to the disruption of the activity of the company caused by any malfunction of the IS Organization.
- Valuable papers and records – covers the actual cash value of papers and records on the insured premises, against direct physical loss or damage.
- Errors and omissions – provides legal liability protection in the event that the professional practitioner commits an act, error or omission that results in financial loss to a client.
- Fidelity coverage – usually covers loss from dishonest or fraudulent acts by employees.
- Media transportation – provides coverage for potential loss or damage to media in transit to off-premises information processing facilities.

To assess the **post event BCP compliance** by the concerned office, I would conduct users/staff interviews and assess related documentary evidence to check:

✓ Whether the role and responsibilities assigned to various individuals, were duly carried out?
✓ Whether the action plans forming part of the BCP were carried out as envisaged?
✓ Whether the services were restored within the expected time as specified in the BCP?
✓ Were appropriate mitigating exercises carried out?

Data Owners are generally the top two layers of management such as directors and managers. They are responsible for using information for running and controlling the business. Their security responsibilities include authorizing access, ensuring access rules are updated whenever there is a change of personnel and regularly reviewing access rules relating to the data for which they are responsible.
Data Custodians are responsible for storing and safeguarding the data and include IS personnel, such as sub-system analysts and computer operators etc.

Questionnaire to assess the controls implemented by WFL in the given areas is as follows:

Water damage controls

□ Whether water proof ceilings and walls have been built at all important places such as data centre, document storage room etc.?

□ Whether a proper drainage system exists in the premises, especially at those places where water-based fire extinguishers are installed?

□ Whether critical IT assets, important documents and archiving records are placed in rooms with raised floors?

□ Whether water alarms are installed at important places?

 If WFL office is situated in a city where floods or torrential rains are likely, whether all material information system assets are placed above water levels (2nd or 3rd floor etc.)

 Whether hardware devices are covered with protective covers when not in use?

 Whether documents are placed in water proof cabinets when not in use?

 Whether computers, servers or client documents are stored just below ceiling or split AC units?

Energy variations controls

 Whether voltage regulators (stabiliser) and circuit breakers are used?

 Whether important data entry systems and servers are supported by UPS?

 Whether standby generator of appropriate capacity is available?

 Whether electrical fittings and equipment meet acceptable quality standards?

 Whether periodic servicing and maintenance of electrical fittings and equipment including UPS and generator is performed?

 Whether generator is always kept fueled?

Terrorist activities controls

 Whether appropriate assessment of the likelihood and vulnerability of the WFL's office to terrorist activity (based on its location etc.) has been carried out?

 Whether proper plan for safeguards to be employed has been prepared by a knowledgeable professional?

 Whether all safeguards as envisaged in the plan have been implemented?

 Whether numbers of local police office, ranger's office, fire brigade, hospitals and ambulance services are displayed visibly in the office?

 Whether periodic drills are held to train the staff to cope with terrorist attack situation?

 Whether

 WFL's office is guarded by armed personnel?

 there is walk through gate at the physical entrance of WFL's office?

 CCTV cameras are installed and live monitoring of critical places is done using CCTV cameras?

 bags and other belongings of staff and visitors have been scanned/checked at the entrance?

 there is a dedicated place for visitors or they are allowed to access anywhere in the office premises?

 vendors' support staff is always escorted within the office premises?

 visitors are required to wear visitors badges?

 staff is required to wear office identification cards?

 Whether WFL has considered terrorism through internet and placed appropriate controls to protect its information systems?

Common causes of database failures are as follows:

(i) Application program error: Data could be incorrectly updated due to bug/error in application program.

(ii) System software error: An error in OS(operating system), DBMS(data base management system), network management system or a utility program may lead erroneous update or corruption of data held by the database.

(iii) Hardware failure: Data may be lost due to hardware failure or malfunctioning.

(iv) Procedural error: A procedural error made by an operator/user could damage the database.

(b)**Common backup strategies** are as follows:

(i) **Grandfather, father, son strategy**: In this method three sets of backups are recorded i.e., daily, weekly and monthly. The daily or son backups are recorded on week days, the weekly or father backups are recorded on weekends while the monthly or grandfather backup is written on last working day of the month. Son, father and grandfather backups are over-written on weekly, monthly and quarterly basis, respectively. Often one or more of the father/grandfather backup is removed from the site and stored at an offsite for safekeeping and disaster recovery purposes.

(ii) **Mirroring / dual recording / replication:** It involves maintaining two separate copies of the same database at different physical locations. It is a costly system as the data is required to be kept and updated at two different locations/servers.

(iii) **Dumping:** It involves copying of the whole or critical part of the database to a medium from which it can be rewritten. There is no specific frequency of taking the backup.

(iv) **Logging:** In this method the backup of the entire database is not taken each time. Instead, a log is kept in respect of all the events that update, create or delete any record in the database. Three types of logs may be kept i.e. transaction logs, before-image logs and after-image logs. Such logs can be used to update the database in case an updated version is lost.