



Omnitech Disaster Recovery System

Omnitech InfoSolutions Ltd
A/13, Cross Road No.5
Kondivita Road, Marol MIDC
Andheri, Mumbai 400093

White Paper

Introduction

Disaster Recovery Services are a further extension of OMNI Tech's commitment to customer services. The disaster recovery services will greatly reduce unscheduled downtime, provide investment protection, strengthen quality assurance programs, enhance data integrity, and offer total assurances on *Business Continuation*.

OMNITECH will approach systematically while...

- Identifying Business Critical Processes by way of Impact / Risk Analysis
- Identifying weak links in most Critical Hardware and applications
- Offering **Server Consolidation** and redundancy management solutions to remove single point of failures (SPOF) in Networks.
- Implementing enterprise wide Storage **Consolidation** and **Backup Management Strategy**.
- Devising efficient Disaster Recovery Technology / Solution needed to take care of critical business processes.
- Developing alternate disaster recovery site (Hot / Cold) for the infrastructure fail-over and Business Continuation.
- Setting up the **Disaster Recovery Plan** (DRP) for the organization to be observed by entire staff in the event of Disaster to get back into the business in predefined period.
- Auditing the DRP on the preset frequency for reliability and forwarding the audit report to the organization.

Disaster Recovery Planning, a need of today's business

A disaster recovery plan is a statement of actions to be taken before, during, and after a disaster. Disaster recovery planning (DRP) can be defined as the development of a comprehensive plan that addresses any type of event that holds the potential of data loss. By planning how your company will respond in the event of a disaster, you ensure that your company can:

- Maintain business continuity
- Protect critical data
- Minimize the impact of a disaster
- Use company resources most effectively

Need for Disaster Recovery Planning

- The ability to quickly recover from a disaster is vital to the survival of a business
- Advances in technology have made disaster recovery a necessity.
- Downtime can result in huge financial losses.
- Service level agreements (SLAs) make business continuity a contractual obligation.

This service will help Organizations in the following areas:

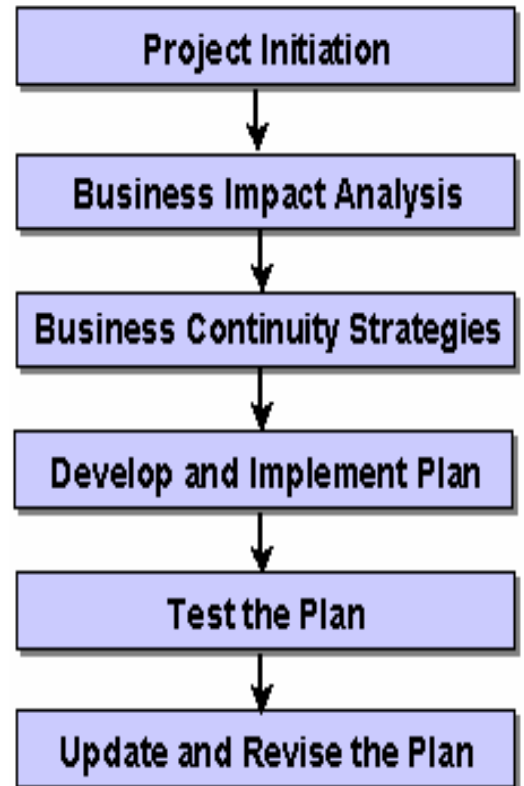
- Identify critical systems, processes and functions
- Assess the economic impact of an IT disruption on the functional areas of an organization.
- Establish the critical time frames or "windows of vulnerability" to the organization.
- Assess the "threshold" or the length of time that the enterprise can
- Manage without access to the systems and services, without adversely affecting the business
- Establish priorities and sequences that need to be followed to restore critical applications and functions.

Omnitech Disaster Recovery Planning Methodology

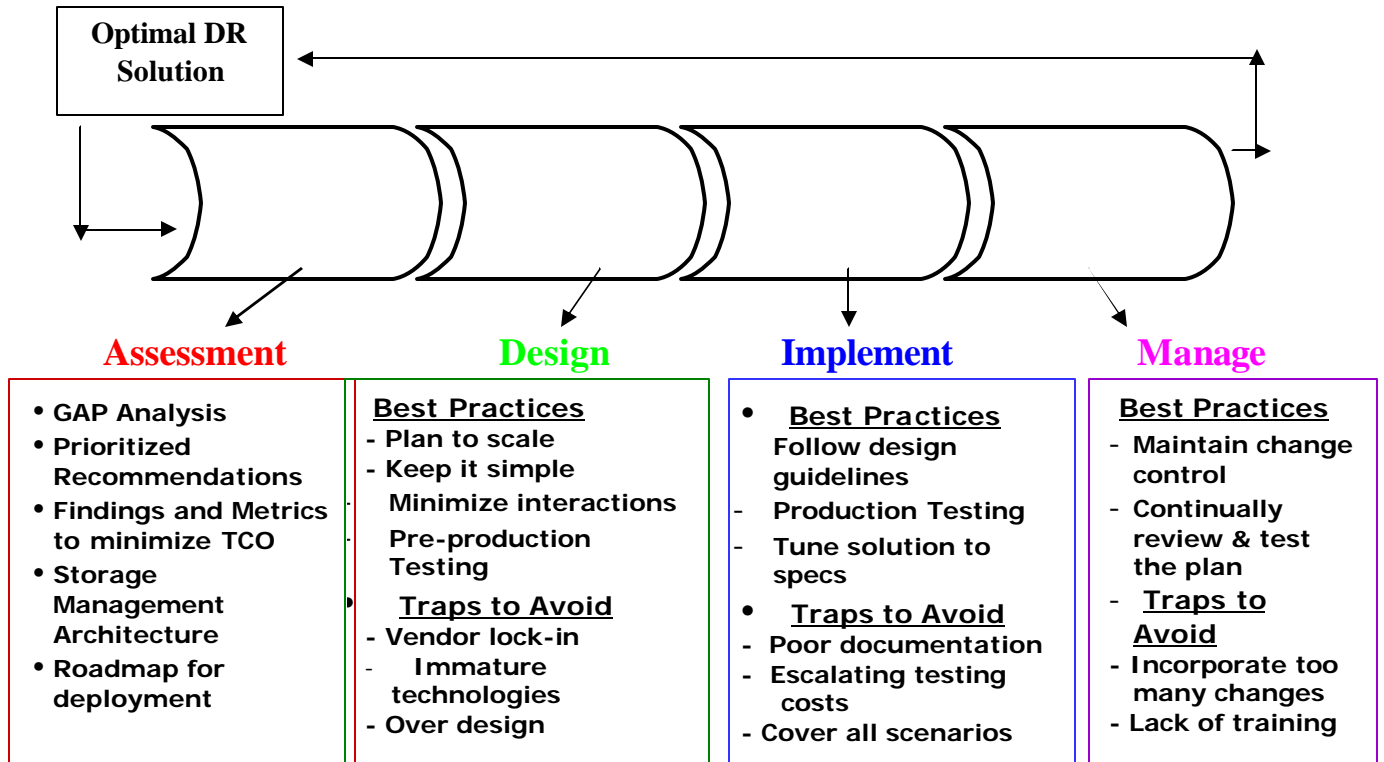
During the Disaster Recovery Planning Omnitech DR Specialist will be forming a **planning team** and **Recovery team** out of the internal staff members. These teams along with Omnitech DR Specialist will take it forward while understanding the critical business processes of the organization and documenting an appropriate recovery plan through **Risk Analysis**.

As a Project initiation initiative, higher Management support will be solicited and DR strategies will be discussed. Management is updated on the DR project through regular project reviews and reports.

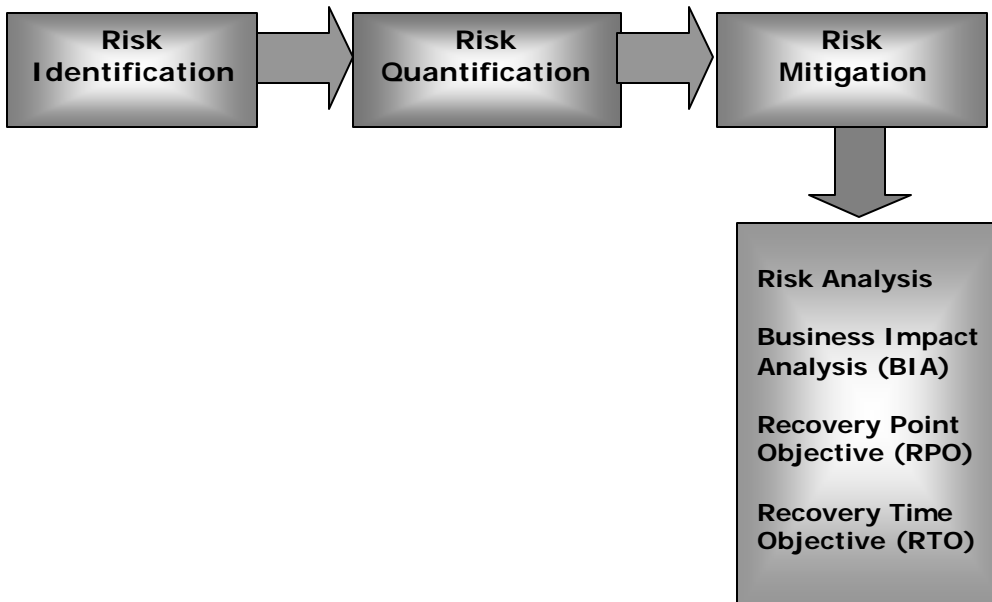
Approved plan is implemented and tested for the different mock scenarios and listed disasters.



Disaster Recovery Planning Stages



Risk Analysis flowchart



Risk Identification

A **process of Risk Identification** is important to enable you to quantify the costs of and mitigate the effects of risks to your operational infrastructure.

During this process possibilities of different disaster are considered which can affect the main site of operation and cause unplanned outage. The considerations are based on historical evidences of natural disaster, Single Point of Failures (SPOF) in the power and networks, Data Recovery and storage policies and known technical disasters like viruses.

The effect of these possible disasters on different business critical processes is identified and the action plan is prioritized depending upon quantification of the impact.

Risk Quantification

The next stage of this process is to quantify the impact of operational interruptions: both tangible and intangible financial exposure. This stage is often referred to as a **Business Impact Analysis (BIA)**. This is a direct cost incurred because of unavailability of system

The output of the BIA includes the maximum acceptable length of time that can lapse before the lack of a business function severely affects the business enterprise, called as **Recovery Time Objective (RTO)** and minimum currency of data lag acceptable to recover back into the business called as **Recovery Point Objective**.

The results of the BIA offers a list of Business Processes dependent on the different IT functions and the amount of tangible losses that will be made if those processes are not recovered within specified time frame (RTO / RPO). These results are utilized further to mitigate the risk by designing the solutions depending on BIA / RPO / RTO

Risk Mitigation

Risk mitigation is an **alternative to minimize operational disruptions**. After detailing down the different business critical processes and the impact of such disaster on the Businesses, a details solution is prepared which offers an alternate path to operate the business processes till the actual operations are restored. Risk Mitigation the solutions are based on the outcome of Business Impact Analysis, RTO and RPO values derived. Normally the solutions are pivotal around three areas.

- **Back up Management**
- **Equipment Fail over (Redundancy)**
- **Infrastructure Fail over (Redundancy)**

Disaster Recovery Levels and Solutions

The different information available after the **Risk analysis** is processed to prepare for complying different levels of Disaster Recovery. *Savior* will start addressing needs for graduating the DR plan to achieve different levels of DR compliance. During the DR compliance program different technologies are applied for appropriate solutions

- **Disaster Recovery Level I:** Storage consolidation, Policy based strategic Backup Management, Backup strategies and tape vaulting facility Is planned and implemented.
- **Disaster Recovery Level II:** Most of the Servers and Active Network Components are critical components of the operations. Single point of failures in such components can raise high level of Disasters and may bring the entire Business to halt. In DR Level II redundancy path is designed for such Components to avoid total disruption. Result of the **Risk Mitigation** offers different redundancy designs for such critical components of the Network. While graduating for this level all single point of Failures are treated for the redundancy planning.
- **Disaster Recovery Level III:** In the final stage of the Disaster Recovery Primary site is offered an alternate site of operation to undertake Business Critical Processes within the stipulated time of Recovery (RTO). While setting up Disaster Recovery site an appropriate data recovery solution is defined to satisfy the needs of RPO and RTO.

Disaster Recovery Plan Implementation

Based on the results of the Risk Analysis an appropriate DR solution is implemented and all the DR levels are tested.

A department / Process wise comprehensive action plan is prepared as to what are the different steps to be taken before, during and after Disaster. Disaster Recovery Plan will be

- Covering all the business critical departments and the processes
- Simple to understand and easily available while disaster occurs
- Undertaking all the liabilities generating out of regulating body, contractual penalties etc
- Known to internal staff members (DR execution team) through training
- Scalable as the business processes changes
- Version controlled

On preparation of the tentative DR plan it is tabled on to Management for the detailed discussions and approval. All the impacts mentioned in Business Impact Analysis is tested on the DR plan.

Final Approved plan is used for the implementation of Disaster Recovery Plan. The Implementation Stages are as follows

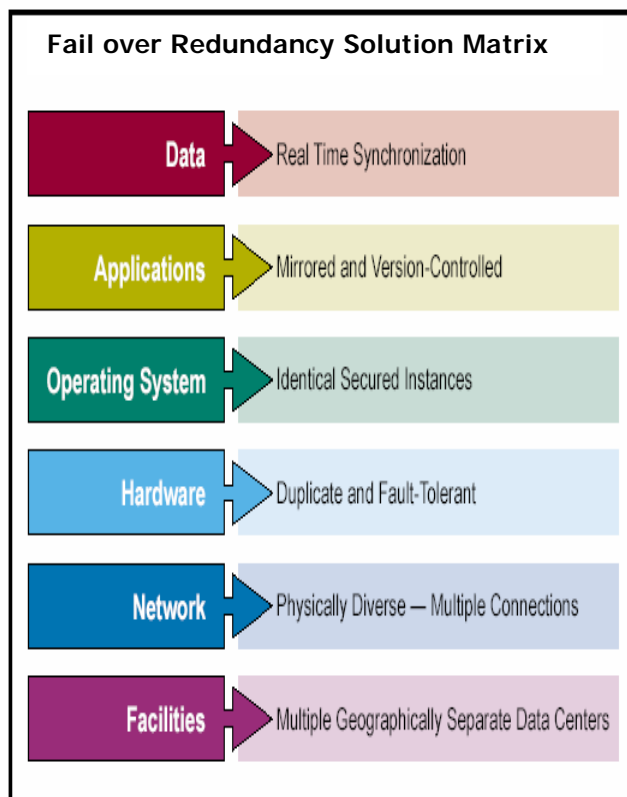
1. The DR Execution team is trained on how to read the plan. The version-controlled copy is distributed to all the Disaster Recovery team members. The same copy is also available at the strategic locations like Server room.
2. The Plan tested for the operation by the team.
3. The Mock Disaster session is tried and the expected results are verified. The final results are forwarded to Management in the review meeting

Testing the DR Plan and Management

So as to ensure that the what ever the objectives set while implementing the DR plan are achieved at all time especially when the Disaster strikes, it very essential that the DR plan is tested for it's reliability of operations.

- Reliable working of the Documented DR plan as per the set norms.
- Amendment of plan aligning new additional business processes
- Training the Organization Staff for DR plan execution
- Preparing the Audit report after the Dry Run on Disaster similar situation

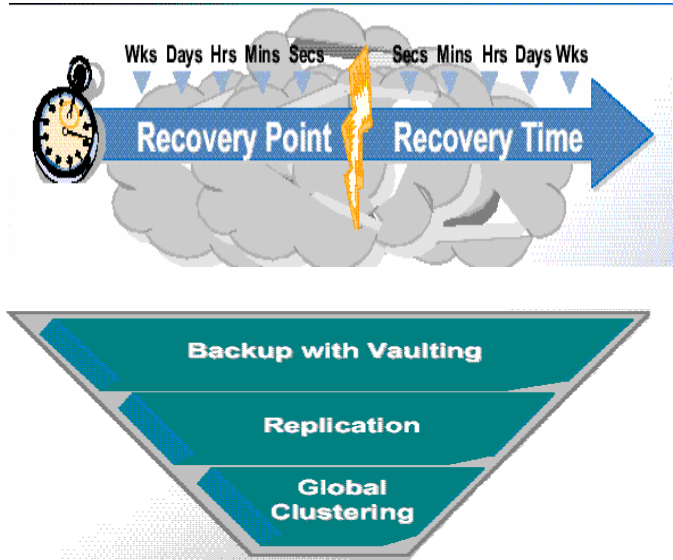
Disaster Recovery Solutions



Disaster Recovery Solution will be addressing to the basic fact that the customer's all the Business Critical Processes will be operative during and after the Disaster is over.

As mentioned in the figure, the solution will ensure the fail over redundancy of **Data, Application, Operating System, Hardware, Network and facilities (entire infrastructure)**

The type of solutions will vary depending upon the Recovery Objective Point (RPO), the data lag allowed to start the operation and Recovery Time Objective (RTO), amount of time required to



The technologies applied to achieve required RPO and RTO will involve Online Backups, Data Vaulting, Server and Network redundancy, Synchronous / Asynchronous Data Replication, Clustering (Local / global), Hot / Cold Mirrored Sites and many more.

During the Impact Analysis Savior *team* will define RPO / RTO values and articulate appropriate solution to satisfy them. While designing the solution it is ensured that the selection of technology / Solution will

- Scale up horizontally / vertically as the nature and volume of the business changes
- Operate reliably in the odd events of disaster
- Accept heterogeneous platform for better interpretability
- Offer higher Return On Investment (ROI)

Disaster Recovery and Business Continuity Services

A. Consulting

1. Business Impact and Risk Analysis

It is important that enterprises assess the impact and consequences resulting from the loss of information and IT services. The cost of implementing and managing a disaster recovery solution should be based on the impact that such disruption would have on the business. Typically, “business impact and risk analysis” form the starting point for the disaster recovery planning in an enterprise.

Any event that can cause a critical resource or a service to be unavailable to users is a risk. A systematic analysis of the critical resources and the associated risks will indicate the impact that the non-availability will have on the business.

This service helps Organization in the following areas.....

- Identify critical systems, processes and functions
- Assess the economic impact of an IT disruption on the functional areas of an organization.
- Establish the critical time frames or "windows of vulnerability" to the Organization.
- Assess the “threshold” or the length of time that the enterprise can Manage without access to the systems and services, without adversely Affecting the business
- Establish priorities and sequences that need to be followed to Restore critical applications and functions.

B. DISASTER RECOVERY PLANNING (DRP)

Disaster Recovery Planning Services will be one step ahead of the Consulting Services. The finding of Risk Analysis is framed in the action plan to ensure that the all the business processes continue to operate during and after disaster has occurred. The total scope is divided into following broad categories

- **DRS Plan Preparation:**

A detailed action plan is prepared to take care of the findings in Risk / Impact analysis. The plan offers stepwise instructions to be observed by the staff members during the Disaster to reinstate back in the operation.

Such DRS plans are prepared after lot of brainstorming sessions with the Organization's Disaster Recovery core project team.

- **DRS Plan Implementation & Testing**

The approved Solution is installed and tested for all different expected results.

The Savior team tests the final report by running the mock Disaster session.

The final results of the Dry run are forwarded to DR Core team for the acceptance.

- **Employee Awareness & Training Programs**

On successful implementation and testing of the DR plan, an awareness program is run across the Organization to make entire Organization about the importance of Disaster Recovery and the basic discipline.

Entire DR core project team and the Recovery (execution) team are trained for the different activities mentioned in the DR plan.

The Dry run is done on the entire plan to ensure that everybody in the recovery team is made enable to understand the DR plan.

- **Current Plan Review & Update**

This service focuses on validating if the existing disaster recovery solution meets current and future business requirement.

Enterprises have the need to review their investments in DR Solution to verify if these Continue to serve the growing needs to the organization. The review phase focuses on two aspects:

- Is the deployment and operations as per plan?
- Will the current DR Solution suffice for future business needs?

Our professionals utilize a structured methodology to conduct the reviews. They will use a mix of interviews and secondary research (documentation available in the enterprise) for these reviews

C. Data Vaulting Services

OMNITECH Infosolution's Savior Vaults provides professional services to help you meet the Disaster Recovery/Business Continuity challenges that every organization faces today. These challenges come in many forms.

Most IT environments are comprised of multi platforms and environments. Our professionals can assist you in sorting through these complexities and help you create a recovery plan that will meet your complex needs and priorities.

Many businesses are constantly updating their technology infrastructure to meet the ever-increasing needs of their business. Savior Vault Services can provide the expertise and resources needed to keep your recovery plan current to minimize your exposure.

Take a good look at your security measures you try to take with business records. Would they survive a natural disaster like flooding or a tornado or a chronic disaster? Do you think your work is protected and disaster cannot wash out your data? If yes, kindly justify. If NO, then I think your search stops here. The storage solution offered by OMNITECH Infosolution's Savior Vaults is the right answer to your query.

Your tapes, disks and documents, which you think, are critical and need an offsite storage solution, and then we can help you. Your tapes and disks are stored in a temperature and humidity controlled environment. We can reconcile with lockers and vaults in which we will store your eminent information. A regular pick up and delivery of tapes and disks is also available at extra costs.

D. Infrastructure Fail over Services

Office space can be rendered inaccessible due to unforeseen, external forces for example, crimes, fires, or gas leaks that cause buildings to be evacuated, power to be shut down, and data centers to become temporarily useless generating the absolute disaster at the infrastructure level. **Infrastructure Fail Over Services** will offer a total Solution to such disasters by offering an alternate infrastructure to Organizations to continue their businesses.

This service helps Organization in the following areas.....

- To reserve the critical executive operational office space to run Business under Disaster
- Availability of equivalent IT setup within stipulated period (RPO/RTO)
- Data Currency available till the last transaction before Disaster stroked
- To Continue all the defined critical business processes to serve their customers

Cool DR Site Services

- Alternative location for storage of customer data
- Off-site/off-line storage of customer provided database backups.
- 24 x 7 x 365 help desk assistance
- On-site disaster recovery consulting services

Hot DR Site Services

- Alternative location in which a customer may access data records from real time replication of their in-house system.
- Off-site storage of customer provided database backups with online access
- Online ad-hoc requests for selected data
- 24.x 7 x 365 help desk assistance
- Performance monitoring services, tuning, and reporting

Omnitech's disaster recovery site will be offering.

- Pre Defined IT setup along with the applications and Data restored
- A space for the your IT team to operate as make shift business house
- Equipped with all the office automation utilities like PCs, telephone, fax, internet, Email
- Centrally air-conditioned with facilities like storage, Cafeteria and rest room
- Operations available 24 hours per day, 7 days per week.
- Round the clock Server, network monitoring and technical support, 365 days a year

Omnitech Disaster Recovery Sites are highly dependable because.

- Fire Protection with, FM 200 based Fire suppression systems
- Video camera surveillance systems, Biometric access & sensors
- On site Power Systems with multiple backup generators feeding a redundant UPS grid to Offer the highest levels of reliability
- Air-Sense State of the art Aspirating smoke detection
- Raised floors
- Security breach alarms
- HVAC temperature control systems
- Managed operations available 24 hours per day, 7 days per week.
- Round the clock network monitoring and technical support, 365 days a year.