INTERACTIVE EURO TECHNOLOGIES

Interactive-Network Disaster Recovery

BACKGROUND

IT systems are vulnerable to a variety of disruptions, ranging from mild (e.g., short-term power outage, disk drive failure) to severe (e.g., terrorism, equipment destruction, fire, acts of God). Much vulnerability may be minimized or eliminated through technical, management, or operational solutions as part of the organization's risk management effort; however, it is virtually impossible to completely eliminate all risks. IET's Disaster Recovery planning is designed to mitigate the risk of network and service unavailability by focusing effective and efficient recovery solutions.

DISASTER RECOVERY PLANNING

Network management encompasses a broad range of activities to identify, control, and mitigate risks to an IT system or Network. First, risk management should identify threats and vulnerabilities so that appropriate controls can be put into place to either prevent incidents from happening or to limit the effects of an incident. These security controls protect an IT system against three classifications of threats.

- Natural—e.g., hurricane, tornado and fire
- Terrorism—e.g., talibans, if they destroy installations and facilities
- Human3—e.g., operator error, sabotage and implant of malicious code
- Environmental—e.g., equipment failure, software error, telecommunications network outage, and electric power failure.

The relationship between identifying and implementing security controls, developing and maintaining the recovery plan, and implementing the recovery plan once the event has occurred.
For example, in many cases, critical resources may reside outside the organization's control (such as electric power or telecommunications), and the organization may be unable to ensure their availability. Responses to these types of incidents involve activities outside the scope of IT recovery planning. Similarly, this document does not address incident response activities associated with preserving evidence for computer forensics analysis following an illegal intrusion, denial-of-service attack, introduction of malicious logic, or other cyber crime.

To effectively determine the specific risks to a Network or IT system during service interruption, a risk assessment of the Network environment is required. A thorough risk assessment should identify the system vulnerabilities, threat, and current controls and attempt to determine the risk based on the likelihood and threat impact. These risks should then be assessed and a risk level assigned (e.g., high, medium, or low). Because risks can vary over time and new risks may replace old ones as a system evolves, the risk management process must by ongoing and dynamic. The person responsible for IT contingency planning must be aware of risks to the system and recognize whether the current contingency plan is able to address residual risks completely and effectively.

IET disaster recovery planning represents a broad scope of activities designed to sustain and recover critical IT services following an emergency. IET disaster recovery planning fits into a much broader emergency preparedness environment that includes Administration and network maintenance process continuity and recovery planning, ultimately, Customer would use a suite of plans to properly prepare response, recovery, and continuity activities for disruptions affecting the organization's network servers, network operations, and the services. Because there is an inherent relationship between a server and the process it supports, there should be coordination between each plan during development and updates to ensure that recovery strategies and supporting resources neither negate each other nor duplicate efforts. The successful completion of such a project requires the close cooperation of management from all areas of Information Systems as well as network areas supported by Information Systems. Senior personnel from Information Systems and user areas must be significantly involved throughout the phase for the planning & implementation process to be successful. In closing, it is important to keep in mind that the aim of the planning process is to:

- Assess existing vulnerabilities;
- Implement disaster avoidance and prevention procedures;
- Develop a comprehensive plan that will enable the organization to react appropriately and in a timely manner if disaster strikes.

Disaster Recovery Program (DRP)

As suggested by its name, the DRP applies to major, usually catastrophic, events that deny access to the network resources & services for an extended period. Frequently, IET DRP refers to an IT-focused plan designed to restore operability of the target systems, applications, or computer facility at an alternate location after an emergency. The DRP scope may overlap that of an IT contingency plan; however, the DRP is narrower in scope and does not address minor disruptions that do not require relocation.

IET follows the following Disaster Recovery Procedures;

- **Program Description**

  Pre-Planning Activities (Project Initiation)

  Vulnerability Assessment and General Definition

  Requirements

  Overall Network Impact Analysis

  Detailed Definition of Requirements

  Plan Development

  Testing Program

  Maintenance Program

  Initial Plan Testing and Plan Implementation

- **Planning Scope and Plan Objectives**
- **Project Organization and Staffing**
- **Project Control**

- **Schedule of Deliverables**
- **Resource Requirements**

The primary objective of a Network Disaster Recovery Plan is to enable an organization IT team to survive a disaster and to reestablish normal network operations. In order to survive, the organization must assure that critical network operations can resume normal processing within a reasonable time frame. Therefore, the goals of the Network Disaster Recovery Plan are to:

- Identify weaknesses and implement a network disaster prevention program;
- Minimize the duration of a serious disruption to network operations;
- Facilitate effective co-ordination of recovery tasks; and
- Reduce the complexity of the recovery effort.

Historically, the data processing function alone has been assigned the responsibility for providing contingency planning. Frequently, this has led to the development of recovery plans to restore computer resources in a manner that is not fully responsive to the needs of the Network supported by those resources. Recovery planning is a Network issue rather than a data processing issue. In today's environment, the effects of long-term operations outage may have a catastrophic impact. The development of a viable recovery strategy must, therefore, be a product not only of the provider's of the organization's data processing, communications and operations centre services, but also the users of those services and management personnel who have responsibility for the protection of the network assets.

The methodology used in this plan, emphasize the following key points:

- Providing management with a comprehensive understanding of the total effort required to develop and maintain an effective recovery plan;
- Obtaining commitment from appropriate professionals to support and participate in the effort;
- Defining recovery requirements from the perspective of functions;
- Documenting the impact of an extended loss to operations and key network functions;
- Focusing appropriately on disaster prevention and impact minimization, as well as orderly recovery;
- Selecting project teams that ensure the proper balance required for plan development;
- Training of the Customer’s network disaster recovery team which will work in coordination with IET.
- Developing a contingency plan that is understandable, easy to use and easy to maintain; and
- Defining how contingency planning considerations must be integrated into ongoing disaster recovery planning and systems restore processes in order for the plan to remain viable over time.

PROGRAM DESCRIPTION

Since recovery planning is a very complex and labor intensive process, it therefore requires redirection of valuable technical staff and information processing resources as well as appropriate funding. In order to minimize the impact such an undertaking would have on scarce resources, the project for the development and implementation of disaster recovery should be part of the organization’s normal planning activities. The IET proposed disaster recovery methodology consists of eight separate phases, as described below.

Phase 1 - Pre-Planning Activities (Project Initiation)

Phase 1 is used to obtain an understanding of the existing and projected computing environment of the organization. This enables the project 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 Committee should be established comprising of both IET and Customer's technical team. The committee should have the overall responsibility for providing direction and guidance to the technical team. The committee should also make all decisions related to the recovery planning effort. 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 process.

Phase 2 - Vulnerability Assessment and General Definition of Requirements

Security and control within an organization is a continuing concern. It is preferable, from an economic and Network strategy perspective, to concentrate on activities that have the effect of reducing the possibility of network 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; security planning and administration; application controls; and personal computers.
- The Security Assessment will enable the project team to improve any existing emergency plans and network 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 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 – Disaster Assessment

A disaster Assessment of all services that are part of the network 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 Servers, devices and other services and facilities; and assess the "pain threshold," that is, the length of time communication units can survive without access to systems, services and facilities. This report will be presented to the Committee. This report identifies critical service functions and the timeframes in which they must be recovered after interruption. The report will 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 network critical functions identified in Phase 3. This profile will include hardware (mainframe, data and voice communications and personal computers), software (vendor supplied, in-house developed, etc.), documentation (DP, user, procedures), outside support (public networks, DP services, etc Recovery Strategies will be based on short term, intermediate term and long term outages.

Phase 5 - Plan Development

During this phase, network disaster 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. Disaster Recovery standards are developed during this phase.

Phase 6 - Testing/Exercising Program

The 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 will be established.

Phase 7 - Maintenance Program

Maintenance of the plans is critical to the success of an actual recovery plan.

The plans must reflect changes to the network environments that are supported by the plans. It is critical that existing change processes are revised to take recovery plan maintenance into account. In areas where change does not exist, network 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 IET professionals 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 disaster recovery strategies are defined, specific testing procedures should be developed to ensure that the written plans are comprehensive and accurate.

PLANNING SCOPE AND PLAN OBJECTIVES

The primary objective of IET’s network disaster recovery planning is to enable Customer’s Team to survive a disaster recovery and to continue normal network operations. In order to survive, the Customer must assure that critical operations can resume/continue normal processing. Throughout the recovery effort, the plan establishes clear lines of authority and prioritizes work efforts. The key objectives of the contingency plan should be to:

- Provide for the safety and well-being of all the equipment on the premises at the time of a disaster;
- Continue critical network operations;
- 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;
- Identify critical lines of network;

Although statistically the probability of a major disaster is remote, the consequences of an occurrence could be catastrophic, both in terms of operational impact and image. IT Management appreciates the implications of an occurrence; therefore, it will assign on-going responsibility for network disaster recovery planning to an employee dedicated to this essential service.

PROJECT ORGANIZATION

The project team organization is designed to maximize the flexibility needed to deal with the implementation of a network disaster recovery plan in the most effective and efficient manner possible. As explained earlier in this document, disaster recovery planning is a complex and labor intensive program. A key factor in the successful development and implementation of recovery and resumption programs is the dedication of a full-time resource to recovery network continuity planning.

Recovery plans must keep pace with these changes. Continuous testing/exercising of plans is essential if the organization wants to ensure that recovery capability is maintained in such an environment. The organization also must ensure that staff with recovery responsibilities, are prepared to execute the plans. This will be achieved with a full-time resource with responsibility for: maintaining plans; coordinating components and full plan tests; training staff with recovery responsibilities; and updating plans to reflect changes to the information processing.

COMMITTEE

The Committee will include representatives from key areas of the organization:

- Information Servers & devices
- Technology Support
- Systems Development
- Network and Operations Services
- Voice/Video Communications
- Network applications & services

PROJECT TEAM

The composition of the Project Team may vary depending on the environments and network services for which plans are developed. The Person/unit responsible for recovery/continuity planning will retain the role of coordinator of testing activities, major plan revisions and maintainer of the Master Plan.

The Core Project Team is automatically part of other project teams. The team leaders represented on the various teams may choose to recommend other senior individuals in their area to represent them or to join specific teams where their expertise will be required for the development of the network disaster recovery plans.

Suggested Core Project Team Composition

- Project Manager
- Computer and Network Operations
- Systems Support
- Voice Network and Communications

Suggested Information Systems/Technology Support Team Composition

- Network & Communications
- Facilities Management
- Network Development and Support
- Database Administration
- Information Systems Security
- Operations
- Network Support
- Network Implementation

SCHEDULE OF DELIVERABLES

The following is a schedule of deliverables by phase that will be developed and delivered as part of this project.

PHASE/DELIVERABLE

Phase 1 - Pre-Planning Activities (Project Initiation)

- Revised Detail Work Plan
- Interview Schedules
- Policy Statement
- Recovery Planning Awareness Program

Phase 2 - Vulnerability Assessment

- Security Assessment Report
- Scope of Planning Effort
- Plan Framework
- Recommendation on Recovery Planning Software
- Implementation of Recovery Planning Software

Phase 3 - Network Impact Analysis

- Network Impact Assessment Report

Phase 4 - Detailed Definition of Requirements

- Recovery Needs Profile
- Plan Scope, Objectives and Assumptions

Phase 5 - Plan Development

- Data Centre Recovery Plan
- Prototype Network Units Resumption Plan
- Recovery Standards

Phase 6 - Testing Program

- Testing Goals
- Testing Strategies
- Testing Procedures

Phase 7 - Maintenance Program

- Maintenance Procedures
- Change Management Recommendations

Phase 8 - Initial Plan Testing and Implementation

- Initial Test Report
- Implementation

RESOURCE REQUIREMENTS

Organizations who have tried to develop disaster plans without dedicating the required resources to the effort have been largely unsuccessful in implementing effective recovery plans. Some organizations, after spending time and money developing recovery plans, have failed in maintaining their recovery capability. This is mostly due to a lack of commitment to keep their plans current or to do regular testing of recovery capabilities. IET management is committed to the development, implementation and maintenance of this program that required resources are freed up during the development cycle and that a resource be dedicated to the on-going network maintenance. Therefore, IET assess the required resources for the development and implementation of network disaster recovery plan. Resource requirements can be divided into three categories, namely:

- Personnel
- Capital Costs
- On-going costs

Network Equipment Disaster Recovery Plan

INTRODUCTION

A disaster recovery plan covers both the hardware and software required to run critical Network applications and the associated processes to transition smoothly in the event of a natural or human-caused disaster. To plan effectively, we need to first assess our mission-critical network processes and associated applications before creating the full disaster recovery plan. This best-practice procedure outlines the steps we need to take to implement a successful disaster recovery plan. We'll look at the following critical steps for best-practice network equipment disaster recovery: Management Awareness, Disaster Recovery Planning, Resiliency and Backup Services, and Vendor Support Services.

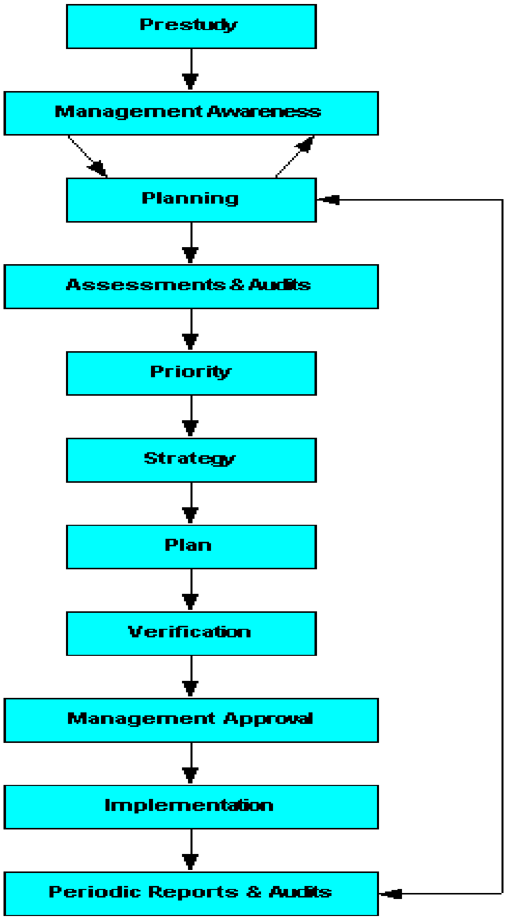
PERFORMANCE INDICATORS FOR DISASTER RECOVERY

Performance indicators provide the mechanism by which we can measure the success of our disaster recovery process and plan. Performance indicators for disaster recovery are somewhat different from those used to measure network performance, because they are a combination of project status and test runs of infrastructure. Indicators of success include:

- Periodic reports from the planning group to senior management.
- Representation of the network design team on the disaster recovery planning team.
- Periodic tests to verify implementation of the disaster recovery plan and reports about gaps and risks.
- A review process that includes the deployment of new solutions.
- Analysis of the disaster recovery handling, effectiveness, and impact on the Network (after a disaster occurs).

HIGH-LEVEL PROCESS FLOW FOR DISASTER RECOVERY

The following diagram outlines IET workflow for managing disaster recovery.



MANAGEMENT AWARENESS

Management Awareness is the first and most important step in creating a successful disaster recovery plan. To obtain the necessary resources and time required from each area of the organization, senior management has to understand and support the Network impacts and risks. Several key tasks are required to achieve management awareness.

IDENTIFY POSSIBLE DISASTER SCENARIOS

First, IET team shall identify the top ten disasters and shall analyze their impact on the network. Analysis would cover effects on communications with suppliers and customers, the impact on operations, and disruption on key network processes. IET team shall complete this pre-study in advance of the disaster recovery planning process, knowing that it will require additional verification during the planning process.

The following are examples of possible disasters: Viruses, Hardware failure, Denial of services, fire, storm, water, earthquake, war, terrorist attacks and other crime, cold winter weather, extreme heat, airplane crash (loss of key staff), and avalanche. The possibility of each scenario depends on factors such as geographical location and political stability.

Assess the impact of a disaster on Network from both a financial and physical (infrastructure) perspective by asking the following questions:

- How much of the network resources could be lost?
- What are the total costs?
- What efforts are required to rebuild?
- How long will it take to recover?
- What is the impact on the overall network?
- How are users requirements, what is the impact on them?

DISASTER RECOVER PLANNING PROCESS

In the disaster recovery planning stage, team shall identify the mission-critical, important, and less-important processes, systems, and services in the Network and put in place plans to ensure these are protected against the effects of a disaster. Key elements of disaster recovery planning include the following:

- Establish a planning group.
- Perform risk assessments and audits.
- Establish priorities for the network and applications.
- Develop recovery strategies.
- Prepare an up-to-date inventory and documentation of the plan.
- Develop verification criteria and procedures.
- Implement the plan.

ESTABLISH A PLANNING GROUP

Establish a planning group to manage the development and implementation of the disaster recovery strategy and plan. Key people from each Network unit or operational area should be members of the team, responsible for all disaster recovery activities, planning, and providing regular monthly reports to senior management.

PERFORM RISK ASSESSMENTS AND AUDITS

In order to create the disaster recovery plan, our planning group needs to thoroughly understand the Network and its processes, technology, networks, systems, and services. The disaster recovery planning group should prepare a risk analysis and Network impact analysis that includes at least the top ten potential disasters. The risk analysis should include the worst-case scenario of completely damaged facilities and destroyed resources. It should address geographic situations, current design, lead-times of services, and existing service contracts. Each analysis should also include an estimate on the financial impacts of replacing damaged equipment, drafting additional resources, and setting up extra service contracts.

ESTABLISH PRI

PRIORITIES FOR THE NETWORK AND APPLICATIONS

When IET’s team have analyzed the risks posed to the Network processes from each disaster scenario, assign a priority level to each Network process. Priorities should be based on the following levels:

- Mission Critical: Network or application outage or destruction that would cause an extreme disruption to the Network, cause major legal or financial ramifications, or threaten the health and safety of a person. The targeted system or data requires significant effort to restore, or the restoration process is disruptive to the Network or other systems.

- Important: Network or application outage or destruction that would cause a moderate disruption to the Network, cause minor legal or financial ramifications, or provide problems with access to other systems. The targeted system or data requires a moderate effort to restore, or the restoration process is disruptive to the system.
- Minor: Network or application outage or destruction that would cause a minor disruption to the Network. The targeted systems or network can be easily restored.

DEVELOP RESILIENCY DESIGN AND RECOVERY STRATEGY

Just as the analysis of the Network process determine the priorities of the network, applications, and systems, the same analysis should be applied to Customer's Network Design. The site priorities and location of key services contribute to a fault-tolerant design, with resilience built into the network infrastructure, and services and resources spread over a wide geography. Develop a recovery strategy to cover the practicalities of dealing with a disaster. Such a strategy may be applicable to several scenarios; however, the plan should be assessed against each scenario to identify any actions specific to different disaster types. IET's plan shall address the following: people, facilities, network services, communication equipment, applications, clients and servers, support and maintenance contracts, additional vendor services, lead-time of Telco services, and environmental situations. IET recovery strategy should include the expected down time of services, action plans, and escalation procedures. IET plan should also determine thresholds, such as the minimum level at which can the Network operate, the systems that must have full functionality (all staff must have access), and the systems that can be minimized.

PREPARE UP-TO-DATE INVENTORY AND DOCUMENTATION OF THE PLAN

It is important to keep inventory up-to-date and have a complete list of all locations, devices, vendors, used services, and contact names. The inventory and documentation should be part of the design and implementation process of all solutions.

IET's disaster recovery documentation shall include:

- Complete inventory, including a prioritization of resources.
- Review process structure assessments, audits, and reports.
- Gap and risk analysis based on the outcome of the assessments and audits.
- Implementation plan to eliminate the risks and gaps.
- Disaster recovery plan containing action and escalation procedures.
- Training material.

DEVELOP VERIFICATION CRITERIA AND PROCEDURES

Once team has created a draft of the plan, IET professionals shall create a verification process to prove the disaster recover strategy and, if strategy is already implemented, review and test the implementation. It's important that we test and review the plan frequently. We recommend documenting the verification process and procedures, and designing a proof-of-concept-process. The verification process should include an experience cycle; disaster recovery is based on experience and each disaster has different rules. IET shall call on experts to develop and prove the concept, and product vendors to design and verify the plan.

IMPLEMENTATION

Now it's time to make some key decisions: How should plan is implemented? Who are the critical staff members, and what are their roles? Leading up to the implementation of plan, try to practice for disaster recovery using roundtable discussions, role playing, or disaster scenario training. Again, it's essential that Customer's Technical Team & concerned authorities approve the disaster recovery and implementation plans.

RESILIENCY AND BACKUP SERVICES

Resiliency and backup services form a key part of disaster recovery, and team shall review these services to make sure they meet the criteria for Network disaster recovery plan. IET defines network resiliency as the ability to recover from any network failure or issue whether it is related to a disaster, link, and hardware, design, or network services. A high availability network design is often the foundation for disaster recovery and can be sufficient to handle some minor or local disasters. Key tasks for resiliency planning and backup services include the following:

- Assess the resiliency of the Network, identify gaps and risks.
- Review of existing & current backup services.
- Implement network resiliency and backup services.

ASSESS NETWORK RESILIENCY

IET shall asses the resiliency of the network keeping in focus the following three levels of availability: reliable networks, high-availability networks, and nonstop network environments. Doing so helps prioritize risks, set requirements for higher levels of availability, and identifies the mission-critical elements of the network.
During assessment IET's team will make sure to evaluate the following areas of the Network:

- Network links
  - Carrier diversity
  - Local loop diversity
  - Facilities resiliency
  - Building wiring resiliency

- Hardware resiliency
  - Power, security and disaster
  - Redundant hardware
  - Mean time before replacement (MTTR)
  - Network path availability

- Network design
  - Layer 2 WAN design
  - Layer 2 LAN design
  - Layer 3 IP design

- Network services resiliency
  - DNS resiliency
  - DHCP resiliency
  - Other services resiliency

Disaster Recovery Solution for Data Centre

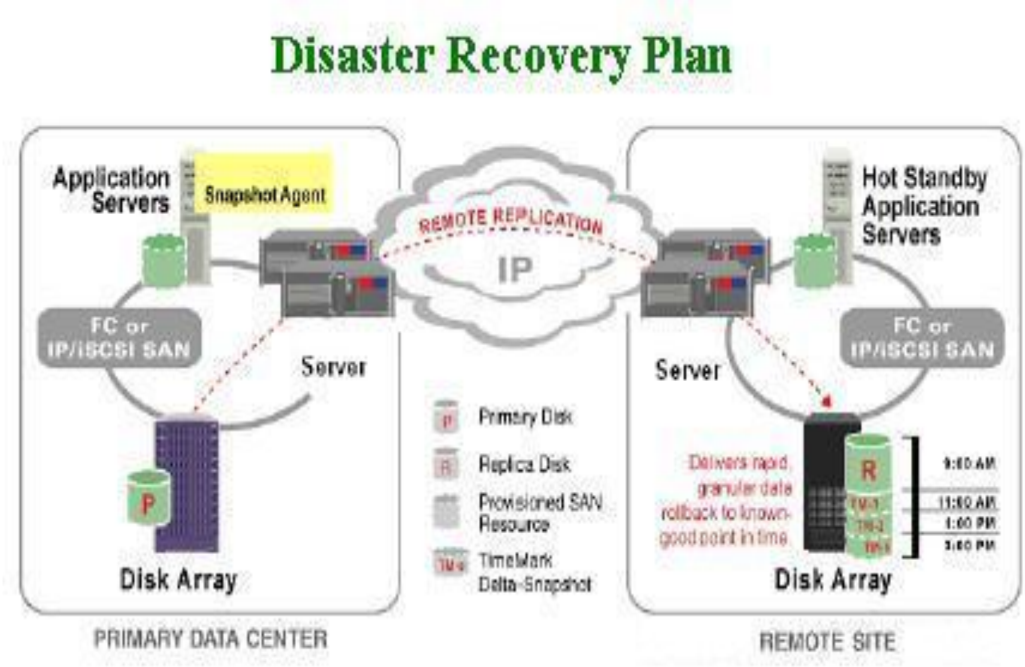
IET Disaster Recovery Solutions facilitate the replication of mission-critical information between data centers, or between remote offices and data centers, via innovative remote replication, asynchronous mirroring, or synchronous mirroring over IP In today's corporate 24x7xForever uptime environment, a practical Disaster Recovery (DR) solution must fulfill the following objectives:

- Address all potential disasters including sudden outages and rolling disasters
- Achieve established recovery time objectives (RTO) and recovery point objectives (RPO)
- Protection of entire data network – from branch offices to the enterprise
- Provide effective data protection during each phase of DR: pre-, during, and post-disaster

Power failures, System failures, Data storage failures, etc., can cause sudden unplanned outages that wreak havoc on day-to-day operations. IET Disaster Recovery Solutions comprised of database-aware, transaction-based Remote Replication for systems; and File Safe and Disk Safe for direct attached storage (DAS) systems. These software tools defend against a comprehensive range of disasters without the expense or integration of specialized storage arrays. Whether it's to achieve established recovery point objectives or recovery time objectives, IET DR Solutions provide rapid resumption of Network in the event of a sudden unplanned outage with minimal data loss, by delivering the functionality required to comprehensively address all phases of a disaster: pre-, during, and post disaster.

KEY BENEFITS

Delivers rapid resumption with minimal data loss addresses both sudden outages and rolling disasters Offers host/OS and storage hardware independence.



Disaster Recovery Planning Issues to Keep in Mind

- back up the data on a regular basis?
- copy the system to the same place every time, over writing the previous copy?
- keep a copy off site?
- backup the data to a server which in turn is backed up by the computer department?
- how long it will take the IT department to retrieve a server backup? In many cases it will takes days and in some cases weeks.
- test the system to make sure it is a good copy of the software and not corrupted?
- store critical program passwords in a secure place known by technical team of the Customer so that they can get to the program in the event that we are permanently unavailable?
- Is software included in Customer 's Network continuity plan?

Plan to Recover From These Disaster Scenarios

- Nasty programming bug corrupts the data.
- Virus contained on the last four-week worth of backups.
- Fire / water damage / flood / theft / civil disobedience prevent access to the office. Chemical spill prevents access to office.
- Purposeful destruction of data / property by disgruntled employee.
- Hard disk failure resulting in corrupted database.
- Undetected failure of data storage resulting in unusable files
- Defective back-up media

The following is a list of simple procedures for less-critical databases:

Disaster Recovery Planning for Small/Less Critical Software System

- First part of disaster recovery planning is easy - backup database systems on a regular database.
- IET shall maintain a minimum of 3 consecutive copies before overwriting.
- Regular courier to another corporate office
- Establish an offsite backup service with courier pickup (for more critical databases).
- Retain Friday's backup for at least six months
- Every six month retain the most recent backup for permanent offsite storage
- Get the database into corporate data backup system if this is available.
- Save key passwords and a copy of documentation in a secure place known by corporate officers
- Periodically test the backups and the disaster recovery procedure to assure that the software up and running again in a timely fashion.

For larger more critical databases IET always consider the following in recovery plans.

Disaster Recovery Plans for Large, Critical Software System

- Develop a written Network continuity plan.
- Identify roles and responsibilities.
- Identify backup personnel for each role.
- Identify a backup location for the use of customer’s database.

- Consider having reciprocal office sharing agreements with a company in the next town.
- Identify necessary computer hardware configuration and software in case it needs to be replaced. For larger companies have POs already written and ready to go.
- Do a walkthrough of recovery plan.
- Practice a real activation of DRP annually.
- Store the plan and all necessary documentation off site.