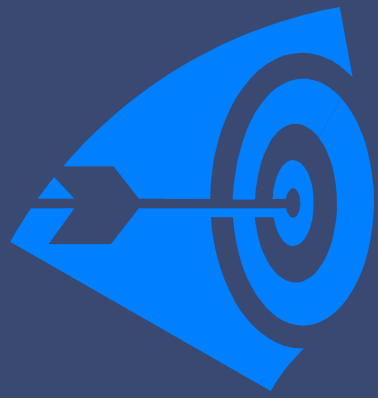
Course: Information Security Management in e-Governance

Day 2

Session 5: Disaster Recovery Planning

Agenda



- Introduction to Disaster Recovery Planning (DRP)
- Need for disaster recovery planning
- Approach for Disaster Recovery Planning
- Key elements in a DRP

Current scenario - Dependence on IT

- IT is becoming the key enabler for many government and public sector organizations in achieving the business objectives
- Many organizations are moving towards mandatory electronic transactions eliminating the manual working methods completely
  - E.g. Ministry of Corporate Affairs (MCA21 Project)
  - E-Procurement initiatives in Andhra Pradesh, Karnataka, DGS & D etc.
  - Passport issuance…
- More and more information is stored electronically
- NeGP is driving IT incubation in all key government sectors/ departments…

Defining a Disaster

As per Principle of Availability of Resources:

- Businesses are run based on the assumption that the current level of resources will not decline.
- Availability addresses the requirement that access to information and resources is available on a timely basis wherever needed to meet business requirements.
- All organizations face the risk that disasters may compromise the availability of resources.

A disaster is defined as any event, which causes unacceptable level of interruption to access for business information, transactions, business operations for an unacceptable period of time. Whenever a disaster strikes, it impacts one or more of the resources, which an organization is employing.

Defining a Disaster (contd..)

A **disaster** may impact in various ways that could affect the organisation's ability to carry on operations. For example, it may:

- not be able to operate from the affected site
- lose critical resources (systems, documents, data)
- lose ability to interact with citizens, businesses, employees, other government agencies..
- not be able to service citizens etc.

Defining a Disaster (contd..)

Few examples of ‘disasters’ in IT Environment

- Organization website is hacked and is inaccessible to people who wish to visit it for a time frame that has an adverse impact on a business
- Application server hosting critical business application is not reachable for a week
- Server room gets flooded with rain water and cables are immersed in water causing short circuit and breakdown of services
- Breakdown of the cooling / UPS units causing high disruption in day to day activities

The Cost/Impact of Disaster..

LEGAL/REGULATORY
- Contractual Requirements
- SLAs
- Regulatory Requirements

PRODUCTIVITY
- Loss Of Productivity
- Employees Impacted

REVENUE
- Direct Loss
- Deferred Losses
- Compensatory Payments
- Lost Future Revenue
- Billing Losses
- Investment Losses

REPUTATION
- Customers
- Suppliers
- Business Partners
- Etc.

FINANCIAL PERFORMANCE
- Revenue Recognition
- Cash Flow
- Payment Guarantees

OTHER EXPENSES
- Temporary employees,
- Equipment Rental,
- Overtime,
- Etc.

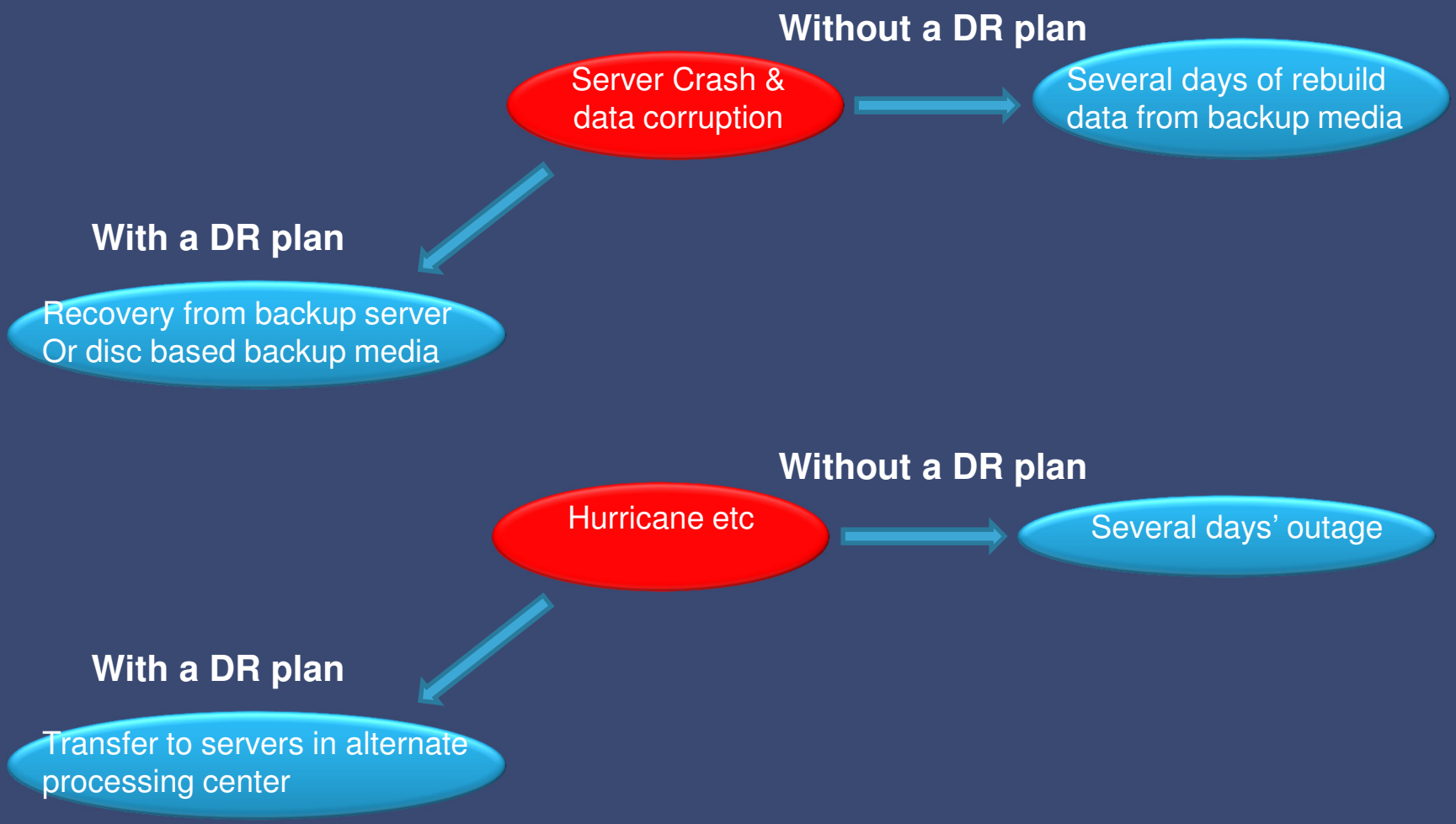
Disaster Recovery Planning

- A Disaster Recovery Plan (DRP) is a set of procedures designed to restore information systems
- Disaster recovery (DR) planning is concerned with preparation for and response when disaster hits.
- DR Planning is:
  - Knowing potential risks to information systems
  - Planning ahead to avoid risks
  - Being prepared in the event a problem occurs
  - Taking the necessary steps to proactively prepare for potential problems
  - Identifying how to respond when a problem occurs…

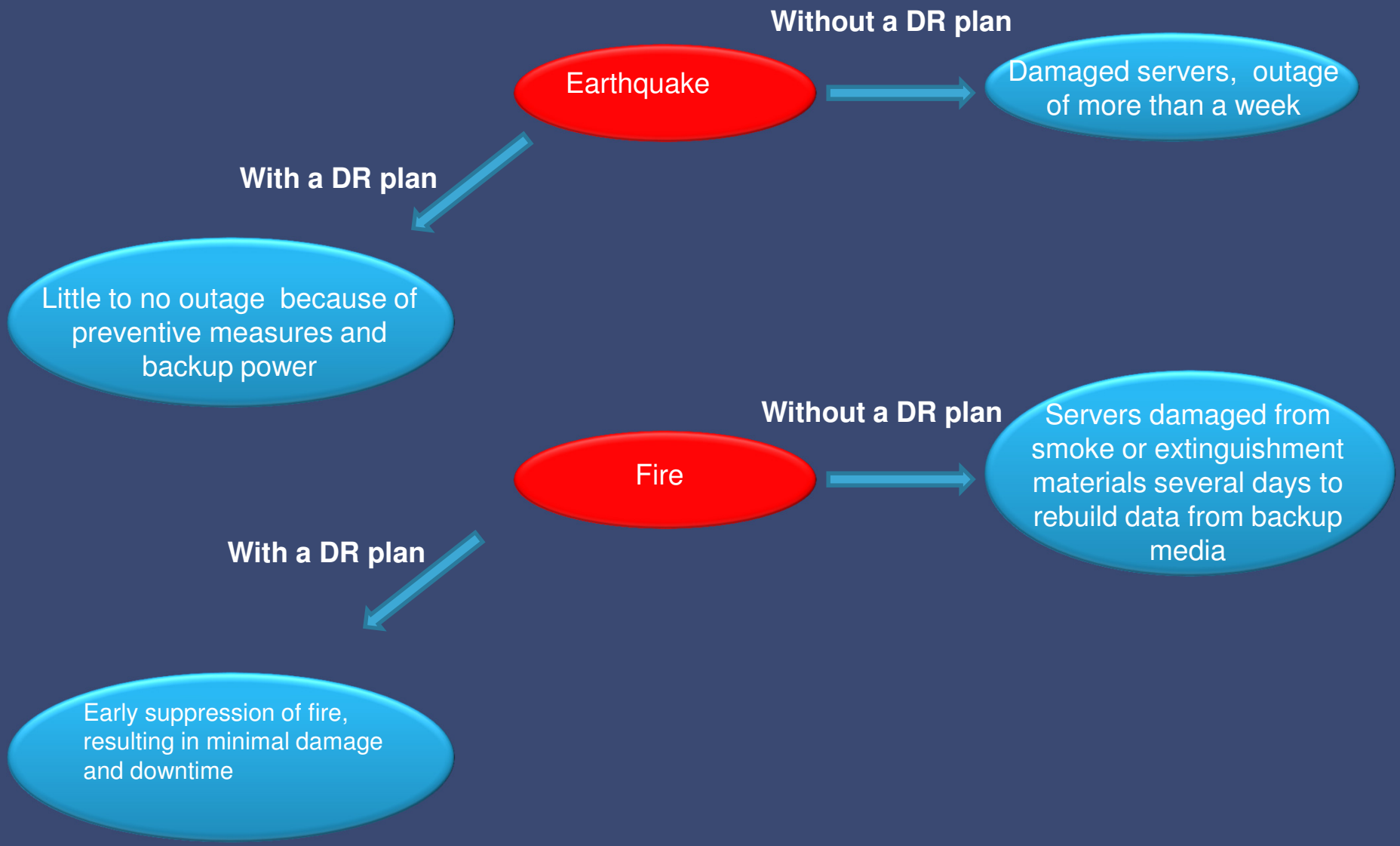
Objectives of Disaster Recovery Plan (DRP)

- Minimize the damage caused to IT enablers and recover them to continue business operations in occurrence of a DRP event.
- Provide a plan of action to facilitate an orderly recovery of critical IT enablers
- Identify key individuals and define their roles and responsibilities, in process of recovering after DRP event
- Catalog probable resources and vendors that could assist in the recovery process.
- Establish general procedures for release of information to employees, customers and stakeholders.

Examples of Events without and with a DR Plan



Examples of Events without and with a DR Plan



Dangerous Excuses for not implementing a Disaster Recovery Plan

- It costs too much money to implement
- Not enough time or resources.
- It will never happen to our company.
- Why bother? We have good data backups.
- We “plan” on implementing one next year !!!

Approach for Development of DRP

Step 1: Risk Assessment: Identification of potential risks in the current IT environment

Step 2: Business Impact Analysis: Analyze the impact of identified risks to the business

Step 3: Strategy Selection: Identification of possible solutions for risk mitigation and selection of appropriate solution based on business needs

Step 4: Plan Development: Documentation of scenarios, solutions, roles and responsibilities for Disaster Recovery

Step 5: Testing and Maintenance: Testing the validity of the plan and keeping the plan updated inline with the changes in IT environment

DRP Approach: Step 1 – Risk Assessment

Risk Assessment consists:

- Health check of existing DR plans (if any)
- Threat/Risk Analysis for IT environment
- Review of existing mitigation programs/measures

DRP Approach: Step 1 – Risk Assessment

Risks in IT environment exists surrounding (illustrative):

- Application Software
- Business Data
- IT Infrastructure – Networks , Computing and Storage infrastructure etc.
- Facilities like Data Centre
- End user environment…

DRP Approach: Step 1 – Risk Assessment

Illustrative Risks surrounding Application Software/Business applications

- Application server crash leading to loss of application software
- Loss of source code/files
- Loss of application design documents
- Lack of support from the software vendor
- Loss of application software change history
- Application software hacked leading to unauthorised transactions
- Loss of training and administration manuals….

DRP Approach: Step 1 – Risk Assessment

Illustrative Risks surrounding Business Data/Database systems

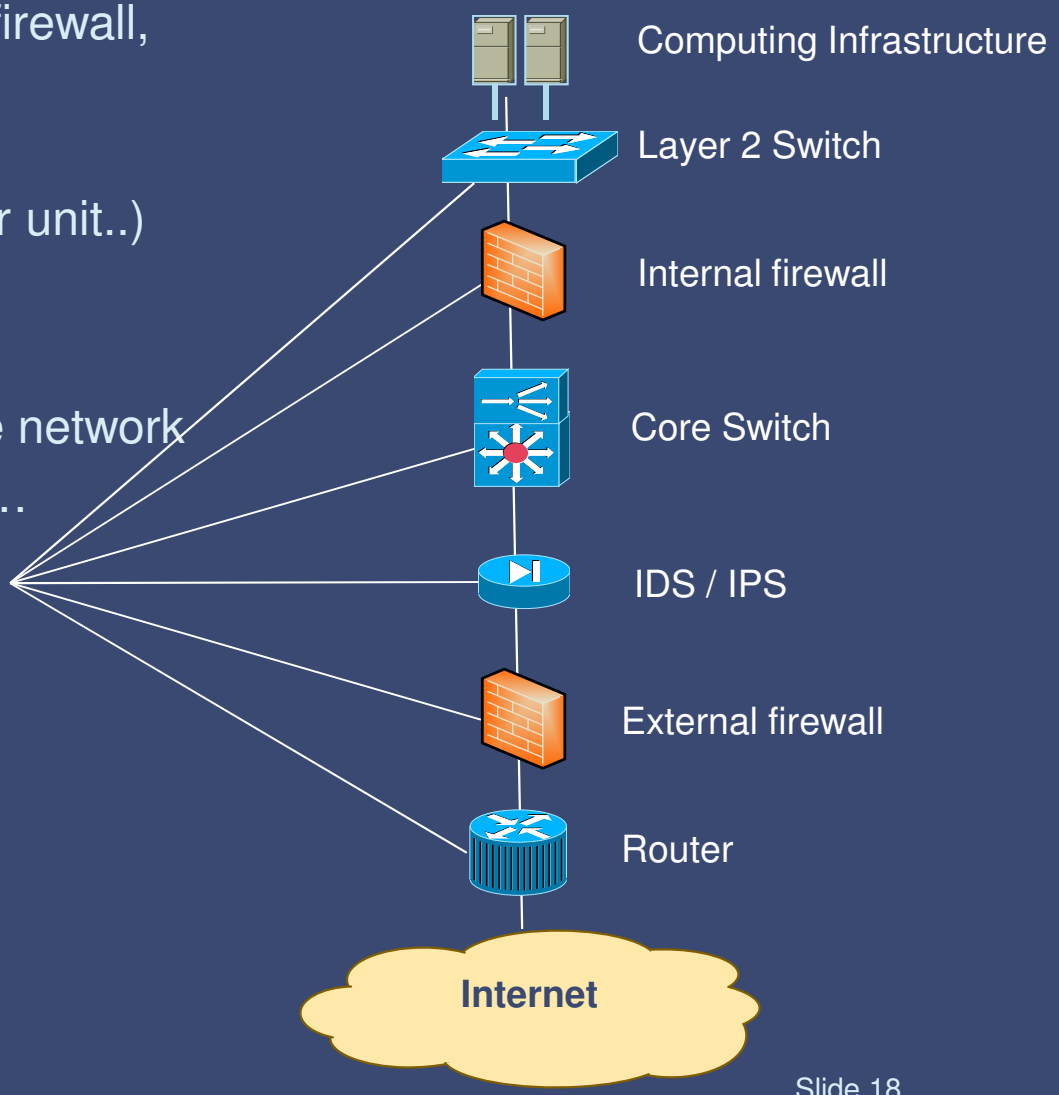
- Database server crash leading to loss of data
- Unable to recover data from data backup tapes
- Unauthorised access/changes to the business data/database systems
- Theft of data/Data falling into wrong hands
- Loss of database design documents…

DRP Approach: Step 1 – Risk Assessment

Illustrative Risks surrounding Network, Computing and Security Infrastructure

- Devise failures (Router, switch, firewall, IPS, Modem.….)
- Module failure…
- Server failure (Disk, RAM, power unit..)
- Network circuits failure
- Cabling failure (LAN and WAN)
- Hacking and penetration into the network
- Denial of Service (DoS) attacks…

Single point of failure



DRP Approach: Step 1 – Risk Assessment

Illustrative Risks surrounding Facilities and support infrastructure

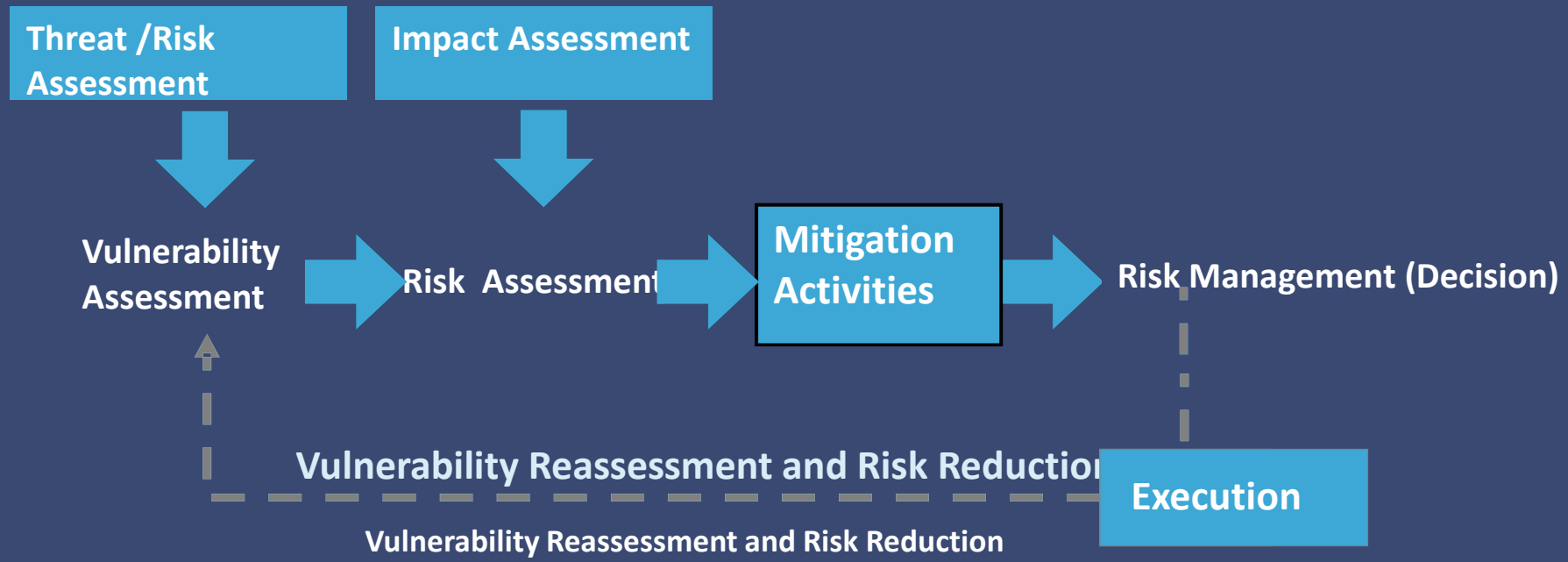
- Discontinued power supply
- Failure in UPS/battery backup
- Generator not working in the need of the hour
- Cooling systems (AC) failure
- Floods and Earth quakes
- Breach in Access control systems
- Fire extinguishers not working…..

DRP Approach: Step 1 – Risk Assessment

Illustrative Risks surrounding End user environment

- PC/Disk failure
- Theft of PCs/Laptops/Data
- Virus attacks
- Installation/usage of unlicensed software
- Printer/Scanner failure…

Risk Assessment – A continuous process



Phase II - Business Impact Analysis

BIA focuses on:

- Identifying the business functions/processes/services
- Impact of the identified risks surrounding Information Systems on the business (functions/processes/services),
- Defining Recovery Time and Recovery Point Objectives

• Provide basis for determining cost effective strategies for risk mitigation

Phase II BIA - Objectives

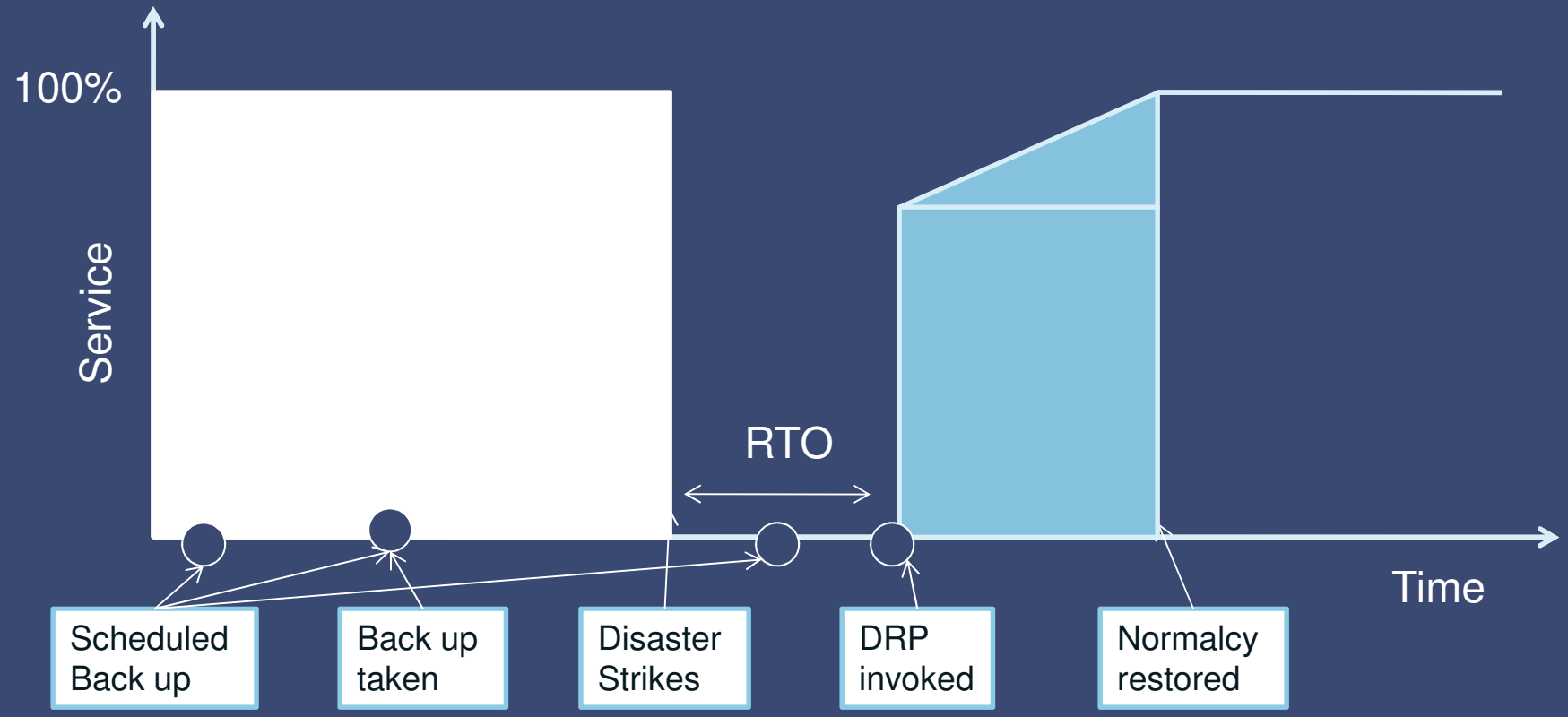
- Determine critical and necessary business functions/ processes and the resource dependencies
- Identify critical computer applications and the associated “outage tolerance”
- Evaluation of impact of identified risks on the business functions/processes
- Estimate the financial and operational impact of the disruption and the required recovery time frame for the critical business functions
- Provide basis for determining cost effective strategies
- Build business case for strategy selection
- Prepare solid foundation for plan development

Phase II BIA – Focus areas

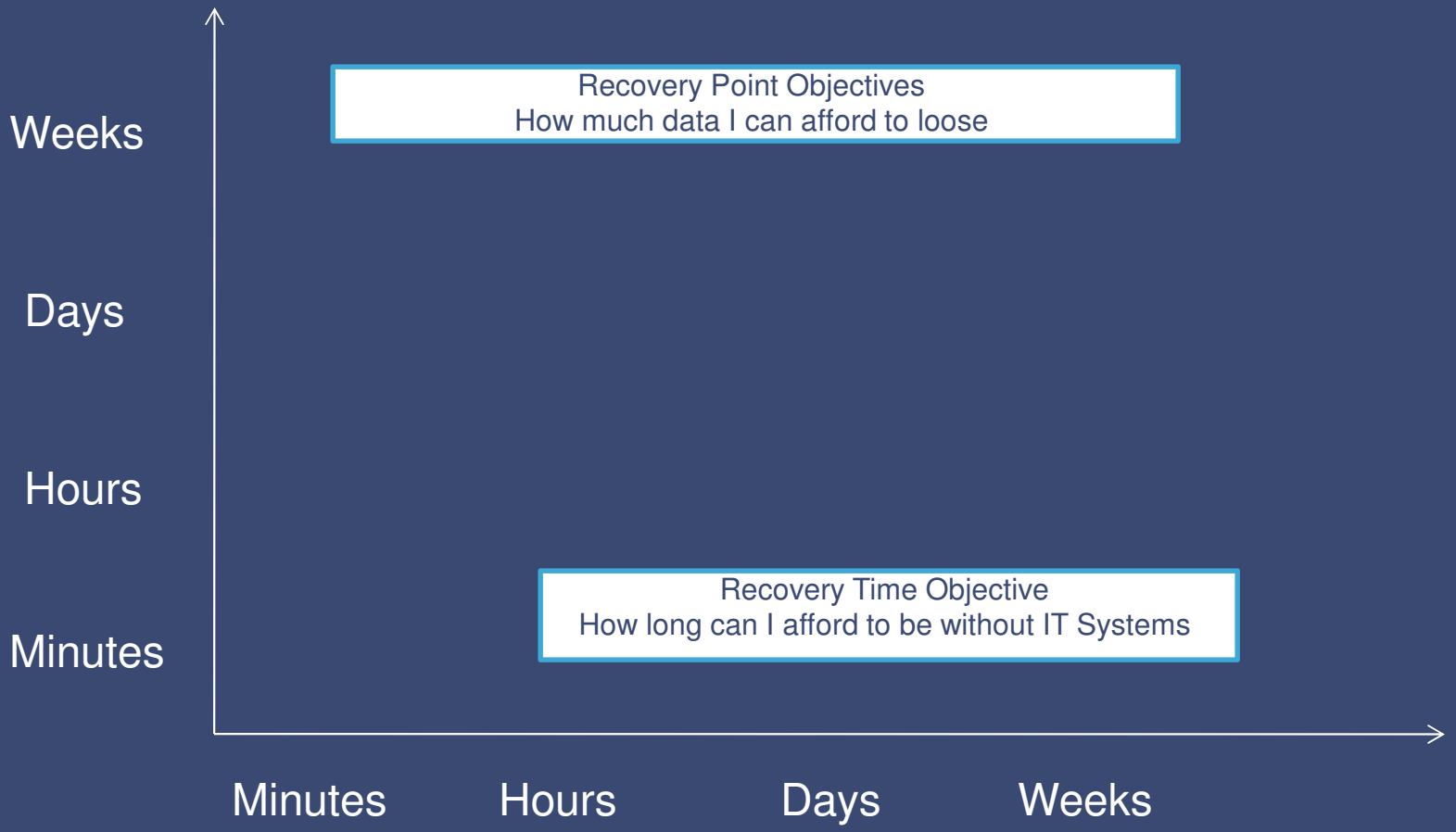
- Describe functions
- Suggest importance
- Describe resources
  - System applications
  - Business Dependencies
- Processing time frames
- Describe contributions
- Estimate impacts due to identified risks
- Describe recovery time frame priorities

Understanding RTO & RPO

- The Recovery Time Objective ***(RTO)*** for an application is the goal for how quickly you need to have that application's information back available after downtime has occurred.
- The Recovery Point Objective ***(RPO)*** for an application describes the point in time to which data must be restored to successfully resume processing (often thought of as time between last backup and when an "event" occurred)



Understanding RTO & RPO



Phase - III: Strategy Selection

- Objective

  Define the action items needed to best protect the organisation and to select the most appropriate recovery solutions for IT systems supporting critical business functions.

- Key Activities
  - Identification of range of solutions/strategies for the identified risks
  - Cost Benefit analysis of identified solutions/strategies based on defined RTO and RPO
  - Strategy selection

Phase III Strategy Selection –
Range of Strategies for Risk Mitigation

We will discuss illustrative strategies available for the following components:

- Application Software
- Data Recovery and Protection
- IT Infrastructure – Networks , Computing and Storage infrastructure etc.
- Facilities
- End user environment..

Phase III Strategy Selection –
Range of Strategies for Risk Mitigation

Range of illustrative strategies for Application Software

- Implement Software Configuration Management tools for version control and source code management
- Backup of application software and source code
- Backup of application design and configuration documents
- Backup of application training, administration manuals
- Updation of application design, configuration, training and administration manuals inline with changes in the software
- Maintenance of Software Change History
- Planning for effective transition management during vendor switch over…

Phase III Strategy Selection –
Range of Strategies for Risk Mitigation

Range of illustrative strategies for Data and Database systems

- Maintain multiple levels of data backup (disk mirroring in server/SAN and backup tapes through tape library)
- Off-site storage of data backup tapes/media
- Data replication at DR site
- Database server configuration and image backup
- Maintain backup of Database design documents…

Phase III Strategy Selection –
Range of Strategies for Risk Mitigation

Range of illustrative strategies for Network and Security components:

- Redundancy at each of the critical network component level (Core router, switch, internet router..)
- Redundancy at network circuit level (network circuits from alternate ISPs)
- Redundancy at each of the critical security component level (firewall, IPS, VPN concentrator..)
- Maintaining spares for the critical infrastructure elements
- Maintain backup of the design, configuration and IP addressing schema files, system images
- Signing SLA with the System Integrators/OEMs for replacement of components inline with RTO/RPO
- Penetrating testing and vulnerability assessment at regular intervals to identify and bridge the information security gaps
- Implementation of network and security monitoring and management tools
- Insurance for the Infrastructure

Phase III Strategy Selection –
Range of Strategies for Risk Mitigation

Range of illustrative strategies for Computing Infrastructure

- Redundancy at the server level
- Maintaining spares for the critical servers and its components
- Maintain backup of the design, configuration and IP addressing schema files, system images
- Implementation of computing infrastructure at alternate site as backup (DR)
- Signing SLA with the System Integrators/OEMs for replacement of components inline with RTO/RPO
- Penetrating testing and vulnerability assessment at regular intervals to identify and bridge the information security gaps
- Implementation of server monitoring and management tools
- Insurance for the Infrastructure

Phase III Strategy Selection –
Range of Strategies for Risk Mitigation

Physical and environmental aspects of IT systems

- Implementation of Disaster Recovery (DR) site
- Power: Redundancy in UPS, power supply from alternate sources/feeds, adequate battery backup, generator set, power supply to the IT equipment through alternate UPS systems
- Cooling: Redundancy in air-conditioning systems
- Security: Video surveillance, Key-card entry controls, Biometric entry controls, Security guards, Hardened facilities, Locking cabinets, Equipment cages
- Environmental controls: Smoke and fire detection, Fire alarms and evacuation, Fire suppression, Fire extinguishers, Sprinkler systems, water detectors
- Insurance for the facilities..

Phase III Strategy Selection –
Range of Strategies for Risk Mitigation

Cold Site

- Have basic environment (power, electric wiring, AC , flooring etc.)
- Ready to receive equipments but do not offer any components at the site in advance
- Activation of the site may take several weeks

Warm Sites

- Partially configured with network connections & selected peripherals equipments such as disk drives , tape drives and controllers but without the main computing infrastructure
- Sometimes equipped with a less powerful central processing unit

Phase III Strategy Selection –
Range of Strategies for Risk Mitigation

Hot site

- Fully configured and ready to be operated in some hours
- Generally intended for emergency operations of a limited time period and not for long extended use
- Components of the DR plan for network connectivity to a hot site over a public switched network should address issuers as redundancy and maintaining sufficient capacity on diverse paths to re-routed path

Reciprocal arrangements

- Arrangement between two or more organizations that possesses similar facilities

User (workstation) Environment - Range of Strategies

- To the greatest extent reasonably possible, use standard configurations for client/server workstations.
- Use imaging technology and tools that can help you quickly build replacement client/server workstations.
  - Test images in a variety of workstation types: In a disaster scenario, you may have to build workstations on hardware platforms that you don't routinely work with.
- Consider a thin-client environment, with client/server software installed on servers, reducing workstations to smart terminals.
  - Thin-client technology enables the organization to centralize client-side software installation, configuration, and maintenance.
- Back up workstation imaging systems.
  - If you can recover those imaging systems in a disaster, you can use them to build new client/server workstations, as needed.

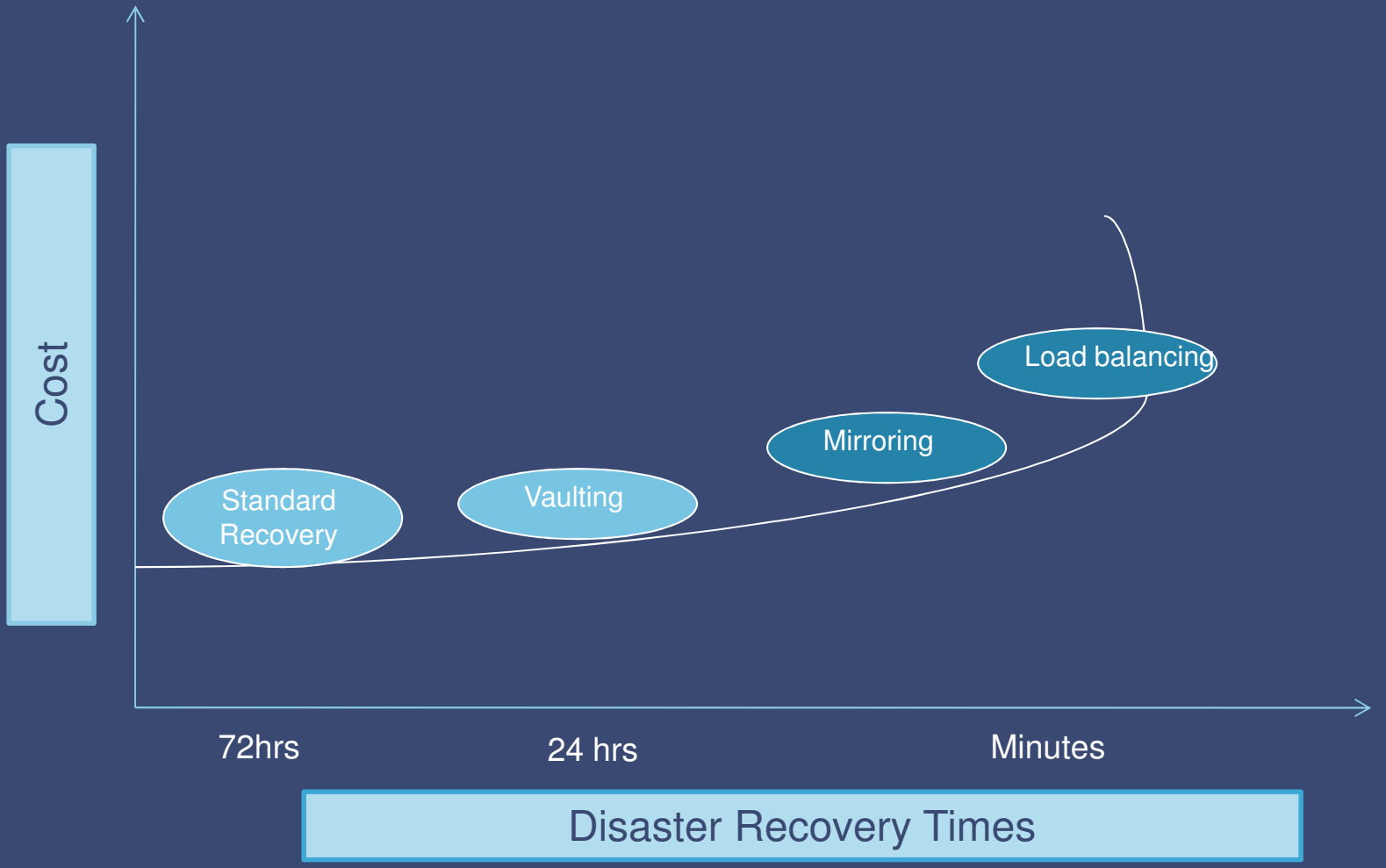
Phase III Strategy Selection –
Range of Strategies for Risk Mitigation

Range of illustrative strategies for End User Environment

- Maintaining end user system images
- Provision for central data backup facilities for end users – for critical data
- Mail server backup
- Maintaining spares for PCs, Printers and other end user computing infrastructure based on failure rates/scenarios
- Signing SLA with the System Integrators/OEMs for replacement of components inline with RTO/RPO

Phase III Strategy Selection –

Cost vs Benefit Analysis of the Strategies - Example



Source : Gartner

Phase III Strategy Selection –

Strategy Selection - Decision

- Alternatives are heavily dependent upon the identified recovery time objectives
- The faster a function is required the more expensive the solution will typically be
- Interdependencies need to be covered during the selection process
- Select the most appropriate recovery strategy

Phase IV: Plan Development

- DR Plan contains an integrated set of procedures and resource information that is used to recover from an event that has caused a disruption to business operations
- It answers questions on responding to a disaster in terms of:
  - Who
  - What
  - When
  - Where
  - Why
  - How
- Plans Contain
  - Each failure scenario has one or more approved alternatives
  - Preparation Plan
    - Advance steps to prepare for the implementation of the alternatives
    - Not all alternatives require preparation
  - Execution Plan
    - The steps to follow if a failure/disaster occurs
    - Includes identification of internal and external dependent groups

Phase IV: Plan Development

1. DISASTER RECOVERY PLANNING OVERVIEW
2. OBJECTIVE OF THE DRP
3. ASSUMPTIONS
4. CLASSIFICATION OF A DRP EVENT
5. SITE DETAILS
6. DRP EVENT HANDLING STRATEGY
7. DRP RECOVERY ORGANISATION
8. FIRST CONTACT AND EVENT REPORTING
9. DECLARATION OF DRP EVENT
10. MEDIA MANAGEMENT PLAN
11. EVACUATION PROCEDURES
12. CRISIS MANAGEMENT TEAM
13. ROLES & RESPONSIBILITIES OF CMT
14. CMT RECOVERY ACTIONS
15. FACILITIES RECOVERY TEAM (FRT)
16. CLASSIFICATIONS OF DRP EVENTS (L1, L2, L3..)
17. DRP ADMINISTRATION
18. PLAN ADMINISTRATION & TESTING
19. PLAN MAINTENANCE
20. PLAN DISTRIBUTION
21. COMPLIANCE AUDIT

Phase IV: Plan Development

1. EMERGENCY CONTACT NUMBERS
2. DETAILED DAMAGE ASSESSMENT AND SALVAGE CONTROL SHEET
3. PROPERTY REMOVAL FORM
4. LIST OF IT VENDORS & SERVICE PROVIDERS
5. LIST OF ADMINSTRATION VENDORS
6. IT HARDWARE INVENTORY
7. INSURANCE DETAILS
8. NETWORK DIAGRAM
9. DRP MAINTENANCE CHECKLIST
10. DRP CHANGE REQUEST FORM

Phase IV: Plan Development – Details for failure Scenario

Failure Scenario	
Possible Causes	

Enablers impacted	Processes Impacted	Departments/Functions impacted

Pre-Events (prevention measures)

Action Steps	Dept Responsible	Individual Responsible

Detection and Escalation

Action Steps	Triggers	Responsibility

Emergency

Action Steps	Dept Responsible	Individual Responsible

Recovery

Action Steps	Dept Responsible	Individual Responsible

Phase V: Testing and Maintenance

Objectives:

- Establish testing and maintenance procedures and timetable
- Testing the plan and procedures
- Finalise and maintain DRP

Benefits:

- Determine if documented recovery strategies & associated recovery procedures are viable to recover critical business functions within their stated recovery time objectives
- Validates planning assumptions
- Identifies strengths and weaknesses
- Provides the opportunity for all parties (IT & other Business Units) to participate together

Testing - Component Testing

- Actual physical exercises designed to assess the readiness and effectiveness of discrete plan elements and recovery activities.
- Isolation of key recovery activities allows team members to focus their efforts while limiting testing expense and resources.
- Effective for identifying and resolving issues that may adversely affect the successful completion of a full interruption test.

Types of Tests

Until you thoroughly test all the recovery procedures, the organization shouldn't expect those procedures to save it from ruin if a disaster strikes.

- **Checklist tests**
  - Preliminary test where the DR plan is reviewed to ensure that it addresses all the procedures and critical areas
- **Simulation test**
  - All the operational and support personnel are expected to perform in case of disaster meet for practice session.
  - Typically goes to the point of relocating to alternate site but does not perform actual recovery
- **Parallel test**
  - Test processes runs parallel to the real processes.
  - Goal is to ensure that critical systems will run at the alternate site if required
- **Full interruption test**
  - Disaster is replicated to the point of ceasing normal production operations. Absolute way to test whether the DR sites works or not .

Thank you…..