



**SUBMITTED BY,
NAME:S.SANTHIYA
REG NO:822221104035
DEPT:CSE
YEAR:III
COLLEGE: UCE-THIRUKKUVALAI**

Building a Disaster Recovery Plan

Learn how to configure replication and test recovery procedures to create a robust disaster recovery plan. Take the right steps before a catastrophe happens.

Replication: The Key to Disaster Recovery

The Importance of Replication

Replication ensures data is available in the event of a disaster. The faster it can be restored, the less impact on business continuity.

Types of Replication

Synchronous and Asynchronous are the two types of replication. Both are important in different scenarios.

Choosing the Right Replication Method

Selecting the appropriate method depends on the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO).

Testing Recovery Procedures: The Proof is in the Testing

1

Importance of Testing

Test all recovery procedures to ensure a successful recovery in the event of a system outage or disaster.

2

Methods for Testing Recovery Procedures

Perform functionality testing, system testing, and full-scale testing. Regular testing ensures updates and enhancements to the DR plan are effective.



3

Challenges and Considerations

Testing is complicated, particularly for complex systems and multiple locations, and requires adaptability to changing conditions and business needs.

Enhancing the Disaster Recovery Plan



Reviewing and Enhancing Existing Procedures

Regular reviews ensure the plan remains effective and up-to-date. Assess procedures to improve efficiency and reduce recovery times.

[illegible]

1. IDENTIFY PEOPLE	3
A. CRISIS COMMUNICATIONS TEAM	3
B. CRISIS SPOKESPERSONS	4
C. STAKEHOLDERS	5
2. IDENTIFY POTENTIAL CRISES AND A PLAN	6
A. BRAINSTORM POTENTIAL CRISES IN ADVANCE	6
B. CRISIS COMMUNICATION RESPONSE PLAN	7
3. IDENTIFY SYSTEMS	8
A. ESTABLISH NOTIFICATION SYSTEMS	8
B. ESTABLISH MONITORING SYSTEMS	8
C. ESTABLISH CRISIS VERIFICATION SYSTEM	8
4. IDENTIFY MESSAGING	9
A. DEVELOP AND USE "HOLDING STATEMENTS"	9
B. KEY MESSAGES	9
5. IDENTIFY KEY LEARNINGS	10
A. POST-CRISIS REVIEW	10

1. IDENTIFY PEOPLE

A. CRISIS COMMUNICATIONS TEAM

Identify the organization's CEO (or head up the team, with the top public relations executive for outside agency or consult advisers. Senior executives, usually the heads of major divisions, should be identified to serve as your organization's Crisis Co-

[illegible]

B. CRISIS SPOKESPERSONS

The good for general communication and good for people should be identified and framed in a chronic, even though you alternate the chronic double about who will group with it and once the data is used. Consider all the different channels of communications, both internal and external, that you may need to know.

CRISIS SPOKESPERSONS			
NAME & TITLE	EXPENSE	PHONE	EMAIL

C. STAKEHOLDERS

Identify and know your stakeholders. Create a complete database of internal and external stakeholders to guarantee that they obtain the needed messages you want them to hear and potentially repeat to other individuals or media outlets, use the Internal/External Stakeholder Communication Plan Template and update it frequently.

STAKEHOLDER COMMUNICATION PLAN					
STAKEHOLDER	POWER / INTEREST	CONTACT METHOD	FREQUENCY	CONTACT INFO	COMMENTS

Developing a Communication Plan

Effective communication is crucial during a disaster. Develop a plan to ensure stakeholders and employees are informed and updated.

The screenshot displays the Opscenter application interface, which is powered by ALERT4. The user is logged in as Jim Paulson, with the role of DR Team Leader. The interface includes a sidebar with navigation links for Status Boards, External Links, Disaster Recovery, Checklists, and Administration-User. The main content area shows a table of applications with columns for Application Name, Application Environment, Responsible Individual, Responsible Organization, Application Id, and Status. Below the table, there is a section for Application Details, which includes fields for Deployment Method, Application Environment, Responsible Organization, and a section for Application Dependencies.

Opscenter
POWERED BY **ALERT4**

User: Jim Paulson
Log Out Help
DR Team Leader

Status Boards
[Contacts \(All\)](#)
[Declarations](#)
[Facilities](#)
[Incidents](#)
[Significant Events](#)

External Links
[CNN](#)
[National Weather Forecasts](#)

Disaster Recovery
[IT Applications](#)
[IT Hosts](#)
[IT Services](#)

Checklists
[Application Recovery](#)

Administration-User
[Change My Password](#)
[My Information](#)

Application Name	Application Environment	Responsible Individual	Responsible Organization	Application Id	Status
Corporate Connection	Finance	Janice Tupolu	IT Operations	15	Available
MCC	Manufacturing	Tom Nicholson	IT Operations	16	Available
OMNI Channel	Infrastructure	Joseph Liebiwitz	IT Operations	24	Recovering
PST	Finance	Michael Paul	IT Operations	17	Available

Application Details

Release Form Clear Save

Deployment Method Manual

Application Environment Finance

Responsible Organization IT Operations

Application Depends on the Following Services

Use this section of the form to display the services on which this application depends.

Status Available

Service	Status	Service Type	Aloc	Allocated Time	Delete
CC Database	Down	Database	0810	15:27:02	
CC Web Server	Down	Web Server	0810	15:27:20	

Implementing Monitoring and Alert Systems

Monitoring and alert software quickly detects system outages and triggers the DR plan. Implement tools to ensure the plan is activated when needed.

Conclusion

1

The Importance of Preparation

Building a disaster recovery plan with robust procedures, replication, testing, and enhancements is essential to business continuity.

2

Continual Improvement

Regular testing and assessment ensure the plan is relevant and up-to-date to meet changing business needs.

3

Effective Communication

Communication and alert systems keep everyone informed and contribute to a successful disaster recovery.