Disaster Recovery Plan for Business Continuity

Milankumar Rana

Department of Information Technology, University of the Cumberlands, Williamsburg, KY 40769, USA
Corresponding author Email: mrana02098@ucumberlands.edu

Abstract: It is prudent to have a Disaster Recovery Plan in place to ensure Business Continuity to be prepared for any disruption that might occur due to unexpected disasters in an organization. This research aims at examining the critical components to consider for a Business Continuity and Disaster Recovery (BCDR) strategy, with a focus of implementing a disaster recovery plan through Azure Cloud. The study frameworks the roles and responsibilities of key stakeholders, the necessary incident response planning, and the procedure and documentation that might help me business continuity. By leveraging the Azure DevOps for automation, the organization can streamline deployment and disaster recovery procedure to ensure timely recovery and minimum downtime through the platforms' Platform as a Service (PaaS), Software as a Service (SaaS), and Infrastructure as a Service (IaaS) solution. This research streamlines the protocol for resource deployment that includes high availability configurations along with failover strategies and real time incident tracking. Planned activities, testing protocols and real time tracking are also examined to check the functionality of the plan and how effective it is to maintain Business Continuity. Significant findings conclude that continuous testing, documentation and process refinement results in better resiliency against failure and proves to be fail safe structured framework for disaster recovery planning by utilizing cloud-based environment.

Keywords: Disaster Recovery, Business Continuity, Business Continuity and Disaster Recovery, Azure, DevOps, Azure Cloud

1. Introduction

Business Continuity and Disaster Recovery planning is critical for any organization to survive and thrive in its business with the best customer experience. Organizations should create a dedicated team to architect, implement, and test overall business continuity. For any organization to achieve this, it requires detailed planning and input from all business unit's managers, stakeholders, directors, and higher-level officers to plan and approve the planning. Implementing the Business Continuity and Disaster Recovery (BCDR) solution depends on various resource deployment models. This research paper focuses on resources deployed in Azure Cloud. The organization has deployed resources through Azure DevOps, so automation is involved in the deployment and the Disaster recovery process. The organization has also deployed various resources via services like Platform as a Service (PAAS), Software as a Service(SAAS), and Infrastructure as a Service (IAAS). The principles that should be followed are:

- If no data retention is needed (state instance), then it should be redeployed in the partner region.
- If data is needed, then the resource itself should be deployed with high availability.
- Name resolution should be used to initiate the failover for resources that are state instances.
- Some resources should be deployed and running in both production and failover regions.

2. Roles and Responsibilities

It is essential to have all Roles and Responsibilities documented and reviewed frequently to update any email or cell number information. This information will help identify key people to alert and remediate the situation during the Disaster. The below table gives us a format to list all required people and their contact details with their responsibilities assigned.

Table 1. Format of table defining roles and responsibilities during disaster recovery.

Name	Role	Responsibilities	Email	Cell
Milan Rana	BCDR Architect	Provide Overall Architecture for Disaster Recovery Implementation	milanrana@xyz.com	111.111.1111
Ryan Drouet	Solution Manager	Responsible for assigning appropriate tasks to team and communicating with Business	ryand@xyz.com	222.222.2222
Alex Grimaud	Business Manager	Identifying business impact and create a plan to communicate with other business regarding SLA response	alex@xyz.com	323.398.3837
Rahul Warhekar	BCDR Engineer	Implement the plan and create backup plan for overall infrastructure deployment	rahul@xyz.com	093.393.3352
Brijeena Shah	Network Engineer	Decision making and testing overall disaster recovery network architecture and testing it	brijeena@xyz.com	888.777.9999
Mrunali J	Test Engineer	Testing BCDR regularly and update to team based on finding	mrunali@xyz.com	848.493.3039
Charm Buffong	Director	Monitoring the impact and providing business requirements to team and communicating to VP and higher-levelorganization about the plan, budgeting	charm@xyz.com	9585.293.1023
Kyle Foster	Project Manager	Collaborating with all team members to share details and create detailed planned documents to present to manager and update regularly based on progress	kyle@xyz.com	676.090.7864

3. Incident Response

Disruption can occur sometimes, so organizations should facilitate an immediate response channel to make them aware of the impact and stand up to a new environment to function normally. Incident responses are tracked through proper tools with all progress updates regarding disruption. It should have a service layer agreement to provide minimum and maximum downtime and its impact on the availability of the resources to the business. The incident should notify a larger group, and appropriately identified team member should be assigned their designated tasks to perform necessary activities. Sub-tasks given to designated team members should be updated immediately regarding progress made, the incident, and communication with the team channel. All leaders from the organization should lead this effort and provide necessary approvals to any blockers that may cause a disaster to bring back operations to normal. The response handling team should keep informing the business about the overall progress and any blockers that may cause further delay. Incident response should involve detailed reports and root cause analysis about why it happened and document it to justify the reason behind it. On the other

hand, the financial risk analysis team should evaluate the economic impact that may occur during downtime. The financial analyst team should be able to estimate the time and revenue loss during business impact.

Table 2. Format of table for incident response reporting.

Item	Incident Number	Incident Manager	Owner
Virtual Machine	INC01	kyle	Milan
Web Application	INC01	Alex	Rahul
Network	INC01	Charm	Sandhya
Database	INC01	Ryan	Kinjal
Data pipelines	INC01	Sri	Srinivas
Automation	INC01	Thomas	Rama
Authentication	INC01	Michael	Kartikay

4. Planned Activities

Once an organization has finalized the architecture and signed off on the implementation, planned activities are crucial to carrying out smooth operations successfully. This should include the objectives and roles of individuals with service layer agreements. Create a runbook that plays a job sequentially for minimum effort and less impact. Document the granular details as much as possible and highlight those to double-check if required. Also, document the training materials to train engineers to frequently perform and test planned activities. Define the deadline to complete tasks for overall architecture. The plan should include the priorities that need to be focused on during backup and categorize those based on resources available and responses about their latest status. Planned activities involve notifying their customer about disruption and the duration it may take to set up the system. This should include distribution lists from different business users and provide up-to-date information about planned activities. On-call support for customers who need immediate assistance with alternate steps to carry out while waiting for the update from the organization. Regular planning and reviewing overall progress help the organization prepare for such an event.

Table 3. Format of table for planned activities in an event of disaster recovery.

Item	Priority	Service Layer Agreement	Test Cases and results	Owner	Data loss	Detail description	Manager
Virtual Machine	High	99.99	Positive	Infrastructure Engineer	0	Recover VM	Guru
Web Application	High	99.99	Positive	Web Developer	0	Restore Application	Shyam
Network	High	99.99	Positive	Network Engineer	0	Paired Region Availability	Alex
Database	High	99.99	Positive	Database Engineer	0	Automatic Backup	Jeetender
Data pipeline	High	99.99	Positive	Devops Engineer	0	Plan Runbook	Ryan
Automation	Medium	99.99	Positive	Devops Engineer	0	Run Automation Script	Kyle
Authentication	High	99.99	Positive	IAM Engineer	0	Test Authentication	Sri

5. **Document History**

Document Describes the index with subject item and details. This document outlines the Architecture Plan, implementation plan, testing results, Recovery plan, and signoff from higher-level team members. Annually, the failover should be tested during an appropriate time for the business. Notifications and timing should be agreed upon by: BCDR Architect, Solution Manager, Business Manager, Directory, and CEO.

The results of this failover should be:

1. Comparison of estimated time to complete each task to actual time.
2. Outline of deviations from documented plan and actual tasks
3. Impact of the failover on production
4. Success of meeting the stated SLA for the application

Six months before the failover, there should be a desktop exercise to evaluate the plan's implementation. The results of this exercise should be:

1. Evaluation of the metrics and the calculations used to estimate time to complete eachtask to actual.
2. Conformation and completeness of the documented plan to the actual tasks that would be performed.
3. Communication of the expected Impact of the failover to clients of the solution
4. Review the SLA and ensure the current plan meets them.

    Update any discrepancy during testing and SLA agreement so that it can be reviewed and updated. The document should be versioned for any update regarding operation, architecture, or any process that needs to be pointed out to the respective item owner.

6. Procedures

Once the organization functions back to normal operations, an organization with a business continuity and disaster recovery plan should prioritize the procedures that include planned activities during the disaster recovery and provide the document to business leaders. This process includes individual tasks performed to mitigate the disaster and who was leading that effort. Statement from business about the disruption cause and impact during these hours. How did the company lead that challenge and handle its customers and investors? Any press release document should be provided to redirect any queries regarding the impact and analysis review. Emergency response documents should be handed over to everyone involved in disaster recovery plans. A process that includes all validations and testing carried out to test all functionality successfully. For the internal team, it is essential to email everyone about the critical steps to further investigate and improve the system for minimum disruption.

Table 4. Format of table to maintain documentation of the event.

Process	Detail Response	Manager
Business Operation	Business operation was stopped due to disaster	Kyle
Disaster Recovery	Team has worked on Recovery operations	Alex
IT operation	All IT operations was affected and recovered	Charm
Incident Center	Incident Center has planned details of all events	Guru
Technical Support	Technical Supports is available all time to help	JP
Human Resource	HR is available for any questions and concerns	Ryan
Website	Websites were restored and tested	Foster
Finance	Financial loss occurred during this event	Michael

7. Conclusion

Overall, this research paper describes the critical information that needs to be collected and assembled to initiate disaster recovery planning. IT disaster recovery involves existing architecture review and design of the disaster recovery architecture that best fits the existing model. Identifying key members for appropriate responsibilities is essential for managers to execute plans and assign roles. Incident response helps categorize the priorities and on-call support from individuals who need to update about the incident and track the progress. Planned activities described in this research paper allow the audience to review the expected activities that need to be performed and evaluated frequently. Document history provides the version of each update and what new things are added to it. This also includes any testing done and documenting the results, finding gaps, and mitigating using appropriate solutions. The procedure, at last, describes how important it is to process the that needs to be carried out once the business is back to normal operations and convey messages to media, investors, and public users about the help they need if any data discrepancy or loss is reported, and they need assistance regarding this.

References

Amaresan, S. (2022, December 30). What Is a Business Continuity Plan? [+ Template & Examples]. https://blog.hubspot.com/. https://blog.hubspot.com/service/business-continuity-plan#how

8 steps for planning your emergency and disaster plan. (2023, December 15). BDC.ca. https://www.bdc.ca/en/articles-tools/business-strategy-planning/manage-business/business-continuity-8-steps-building-plan

IT Disaster Recovery Plan | Ready.gov. (n.d.). https://www.ready.gov/business/emergency-plans/recovery-plan#:~:text=Developing%20an%20IT%20Disaster%20Recovery%20Plan&text=The%20plan%20should%20include%20a,replicate%20and%20reimage%20new%20hardware.

Brush, K., & Crocetti, P. (2022, May 18). disaster recovery plan (DRP). Disaster Recovery. https://www.techtarget.com/searchdisasterrecovery/definition/disaster-recovery-plan

IBM documentation. (n.d.). https://www.ibm.com/docs/en/i/7.3?topic=system-example-disaster-recovery-plan

What is a Disaster Recovery Plan? Definition + Strategies. (n.d.). Druva. https://www.druva.com/glossary/what-is-a-disaster-recovery-plan-definition-and-related-faqs