

## Review Article

## Open Access

## The Best of Both Worlds: A Practical Guide to Hybrid Disaster Recovery for Virtualized Environments with Hyperconverged Infrastructure and Cloud Services

Raja Venkata Sandeep Reddy Davu

Senior Systems Engineer - Virtualization and Cloud Solutions, Texas

### ABSTRACT

Hyperconverged infrastructure and cloud services enable hybrid Disaster Recovery (DR) in virtualized settings, protecting data and keeping enterprises operational. This study examines HCI in virtualized settings, emphasizing easier management, more freedom, and better resource consumption. Comparing old and contemporary disaster recovery approaches shows how difficult it is to handle rising data, speedy recovery, and following the regulations. Mixed DR solutions' adaptability, scalability, and cost-effectiveness are studied. This solution includes cloud-based DR with on-premises HCI. Disaster recovery is discussed in this in-depth look at disasters and corporate operations. Traditional DR is expensive, complicated, and slow to recover. Modern DR issues include rigorous regulations and speedier healing. This study compares recovery time objectives (RTOs) and recovery point objectives (RPOs) with old and new DR systems using graphs to prove that hybrid DR methods are preferable. Implementing a hybrid disaster recovery strategy requires assessment, planning, architecture, deployment, testing, and validation. A resilient DR plan requires regular tests, security safeguards, thorough recording, and constant monitoring. The paper uses graphs and statistics to discuss hybrid DR's benefits, including better RTO and RPO, savings, and easier management. Cloud computing, threat changes, automation, and orchestration are examined for disaster recovery's future. AI-driven disaster recovery solutions with superior failure prediction and recovery optimization are predicted to become more prevalent. The paper concludes that proactive DR planning and ongoing adaptation are essential for firms to be resilient and ready for future shocks.

### \*Corresponding author

Raja Venkata Sandeep Reddy Davu, Senior Systems Engineer - Virtualization and Cloud Solutions, Texas, USA.

**Received:** September 01, 2023; **Accepted:** September 09, 2023; **Published:** September 18, 2023

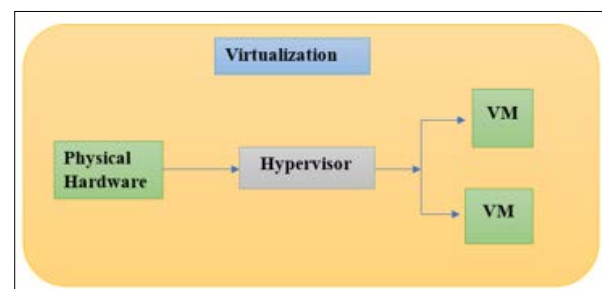
**Keywords:** Hybrid Disaster Recovery, Hyper Converged Infrastructure, Cloud Services, Virtualized Environments, Data Protection, Recovery Time Objective, Recovery Point Objective, Disaster Recovery Testing, Security Compliance, AI-driven DR Solutions.

### Introduction

Modern information technology plans must include disaster recovery (DR) because data is companies' lifeblood. A framework of rules, methods, and technology called "disaster recovery" restores or maintains vital IT infrastructure and systems following an assault. Businesses need disaster recovery (DR) to avoid service outages and data loss from natural disasters. Without a disaster recovery strategy, firms might suffer operational disruptions, financial losses, and brand damage [1]. Protecting company operations has long required traditional DR solutions. Such techniques include tape backups, offshore data storage, and several data centers.

A tape backup writes data to magnetic tape and sends it to a secure offsite storage facility. Tape backups are cheap but sluggish, cumbersome, and fragile. Offsite data storage involves generating copies of data and storing them in other locations to mitigate localized disasters. Despite its reliability, this procedure is expensive and requires careful planning and implementation. Redundant physical data centers keep backup facilities online to continue service after an outage or other disaster. Many organizations find this technique expensive due to the high initial

investment and ongoing maintenance. Due to the inadequacies of older, more conventional disaster recovery (DR) solutions, virtualized environments and Hyper-converged Infrastructure (HCI) have developed as more effective and cheaper alternatives. Servers, storage devices, and networks are digitally represented through "virtualization". Virtualization abstracts hardware resources, making resource allocation more efficient and flexible [2]. This reduces costs, simplifies management, and improves scalability. Hyper-converged infrastructure (HCI) transforms virtualization by integrating processing, storage, and networking into a single software platform. HCI eliminates multi-tiered architectural concerns, simplifying and scaling. HCI advantages include performance, scalability, administrative simplicity, and hardware footprint reduction. HCI is becoming more widespread in modern data centers because it helps organizations manage IT resources.



**Figure 1:** Virtualization Hypervisor Diagram

As organizations implement virtualization and HCI, hybrid disaster recovery, which combines on-premises HCI with cloud services, is becoming increasingly common. Hybrid DR uses on-premises and cloud settings to deliver a strong, scalable, and affordable disaster recovery solution. Integrating HCI with cloud services can improve data security, disaster response, and recovery times. Hybrid disaster recovery solutions often move mission-critical programs and data from on-premises HCIs to the cloud. In a crisis, the cloud may take over operations, ensuring minimum business impact [3]. This strategy improves resilience and saves money by reducing redundant physical infrastructure.

Cloud services' on-demand scalability lets organizations scale disaster recovery capabilities as needed instead of keeping capacity idle. This paper provides a comprehensive guide on building HCI-based cloud services for hybrid disaster recovery in virtualized environments. It will explain disaster recovery, why hybrid DR is superior, and how to apply it. The paper will also include case studies and examples to demonstrate hybrid DR's value and illuminate disaster recovery trends.

### Virtualized Environments And Hyperconverged Infrastructure Virtualized Environments

Due to their flexibility, virtualized environments are an important part of modern IT design. With virtualization, software acts like hardware like storage devices, servers, and network tools. Hypervisors, which are software layers that let multiple virtual machines (VMs) run on a single real host, are often used for this. Hosted hypervisors run code on an operating system, while bare-metal hypervisors run code directly on hardware. Virtualized settings need hypervisors, virtual machines, and networks to work. VMMs are kept separate and safe by hypervisors like VMware ESXi, Microsoft Hyper-V, and KVM [4].

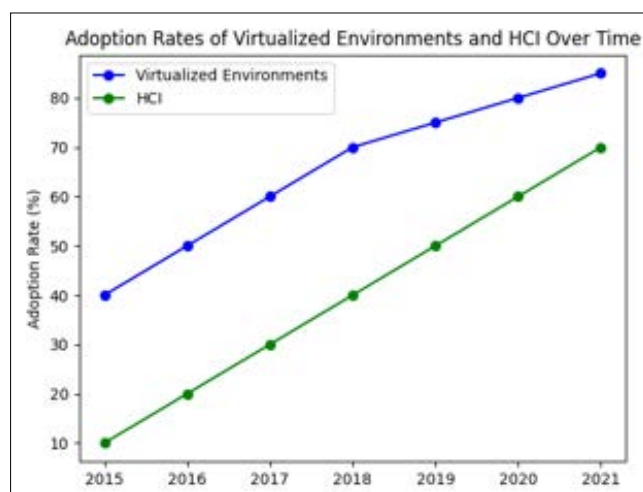
Hardware resources are distributed to VMs by hypervisors. Virtual machines are software simulations of real computers with their own OS and apps. Virtual networks allow virtual machines (VMs) to communicate with each other and external networks by imitating real-world networking gear like switches and routers. Virtualized environments have many benefits. They optimize resource use by letting multiple virtual computers share physical hardware. The consequence is decreased hardware costs and higher usage. Due to its remarkable flexibility, virtualization lets IT managers construct, modify, and decommission virtual machines (VMs). Testing and development environments require fast deployment and iteration, where agility is especially beneficial.

### Hyperconverged Infrastructure (HCI)

Hyper-converged infrastructure (HCI) combines networking, storage, and processing into a single, streamlined system that is run by a single piece of software. Multi-tiered systems make it harder to set up and handle IT infrastructure and HCI makes it easier. The CPU, memory, and storage are all on HCI units. High-speed networks and software-defined management tools let us handle and keep on monitoring all of these nodes as a single system. Businesses can gradually increase the size of their infrastructure by adding nodes to the cluster. This is possible because the combination makes it easy to scale and distribute resources. One set of rules controls all of HCI's computing, storage, and networking tools. This interconnect simplifies data center operations and eliminates control interfaces. Existing HCI alternatives include data backup, disaster recovery, and protection [5]. This simplifies mission-critical IT service management. An HCI infrastructure integrates computation, storage, and networking. This reduces managerial complexity and costs.

Simplifying these processes may allow IT staff to focus on more important duties and goals rather than bug fixes and system reliability. Other benefits of HCI include cost reduction.

The integrated architecture of HCI systems eliminates the need for IT expertise and hardware, lowering currency and operational costs. HCI's pay-as-you-grow strategy lets organizations build infrastructure gradually, ensuring usage-based charges and avoiding large upfront costs. Due to its expandability, HCI is ideal for enterprises with fluctuating IT needs. Companies can simply add storage, computing power, and network capacity to HCI systems by adding servers to a cluster [6]. Businesses can increase their IT systems to handle more workloads. Virtualized settings and HCI implementation frequency are shown in this figure. These technologies are adopted quickly in data centers.



**Figure 2:** Adoption Rates of Virtualized Environments and HCI Over Time

### Fundamentals of Disaster Recovery

#### Definition and Importance of Disaster Recovery

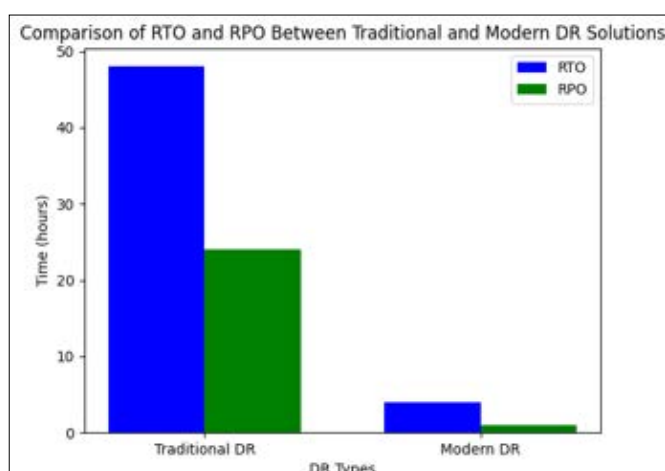
Disaster recovery (DR) is essential to IT system management to restore business and data. Such breaks can be caused by natural disasters like earthquakes, floods, and storms, as well as by cyberattacks, sabotage, or accidentally deleting data, or by technological problems like hardware or software failures [7]. Businesses ensure that their data will be safe and that emergency downtime will be kept to a minimum with disaster recovery. The legitimacy, financial stability, and compliance with regulations of a business all rely on its disaster recovery plans. Tape backups, external storage, and replication are all common ways to handle disaster recovery (DR). Backup tapes copy data to magnetic tape cartridges and store them so that data is safe in case of a local disaster. This method is reliable for long-term storage, but it requires moving tapes and is laborious. The recuperation process can also be lengthy. Offsite storage involves storing essential data elsewhere. This method reduces regional disaster data loss. By replicating data and system states to a secondary site in real time or near-real time, essential information is always available. Even though widely utilized, conventional DR approaches have shortcomings. The equipment, software, and storage space they require are expensive. These systems can also be complex to manage and require IT professionals to organize backups, storage, and recovery.

Traditional DR systems' recovery periods might generate long operational downtime that hurts a company's revenue and productivity.

## Modern DR Challenges

Companies in the digital age face many additional challenges that make catastrophe recovery harder. Due to exponential data growth, more scalable and resilient storage systems and faster recovery methods are needed to prevent downtime. Because businesses rely on digital services and cloud computing, downtime can affect internal procedures and customer satisfaction. Companies must also demonstrate their ability to recover quickly from interruptions and comply with data protection standards as regulatory compliance requirements increase. Modern disaster recovery systems must be effective and fast to recover from data expansion to overcome these challenges and meet regulatory criteria [8]. Businesses must also minimize data loss and recovery times. Since standard DR approaches fail in some areas, more advanced and integrated solutions are used. Check out this graph comparing RTO and RPO to understand how modern DR solutions differ from traditional ones.

Comparison of RTO (Recovery Time Objective) and RPO (Recovery Point Objective) Between Traditional and Modern DR Solutions

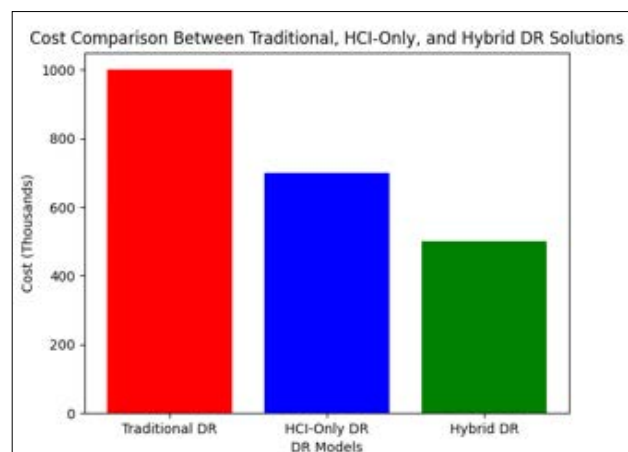


**Figure 3:** Comparison of RTO and RPO between Traditional and Modern Solutions

## Hybrid Disaster Recovery: Combining HCI and Cloud Services Concept of Hybrid DR

Hybrid DR combines cloud-based and on-premises Hyperconverged Infrastructure for flexible and cost-effective disaster recovery. HCI centralizes processing, storage, and networking, simplifying management and providing virtualized environments with scalable resources. Cloud services let organizations expand their DR capabilities beyond on-premises equipment by using the cloud's almost endless processing power and storage capacity. A hybrid DR strategy combines on-premises HCI systems with cloud-based DR solutions like AWS, Azure, or GCP [9].

Businesses may now use the cloud's scalability, regional redundancy, and improved data protection while keeping their local HCI systems' low latency and performance. Hybrid DR has many benefits. By efficiently using on-premises and cloud resources, large physical infrastructure and maintenance costs can be lowered, this reduces costs. They gain flexibility when they can simply swap workloads between local and cloud environments and dynamically assign resources to meet demand. HCI and cloud services increase RTO and RPO, reducing data loss and speeding recovery after an interruption.



**Figure 4:** Cost Comparison between Traditional, HCI-Only, and Hybrid DR Solutions

## Designing a Hybrid Disaster Recovery Strategy

A thorough review and preparation are needed for disaster recovery to work well. Set realistic Recovery Time Objectives (RTOs) and Recovery Point Objectives after figuring out which apps and data are mission-critical. Next, observe the risks and effects. Before making a mixed DR plan, we should figure out which apps and data are essential to the business. We will need to list and value the company's IT assets to do this. It is important for businesses to highlight applications like financial reporting, supply chain management, and customer transactions [10]. To use these programs, we need to find and sort client, financial, and operational info. Risk and effect analysis are done after necessary applications and data have been found. Natural disasters, cyberattacks, technology problems, and mistakes made by people are some of the risks that come with this. Studies of the effects look at how much money these risks cost, how they hurt the image, and how they stop the business from running. Organizations can better control their resources and set priorities for DR efforts when they understand these risks and their effects. For crisis recovery, RTO and RPO are very important. We can measure how long a service can be down before it hurts the business by its reliability, throughput, and availability (RTO). The time-based data loss limit is shown by RPO. Making RTO and RPO goals that are attainable helps make a DR plan that fits the needs of the business and guarantees reliability.

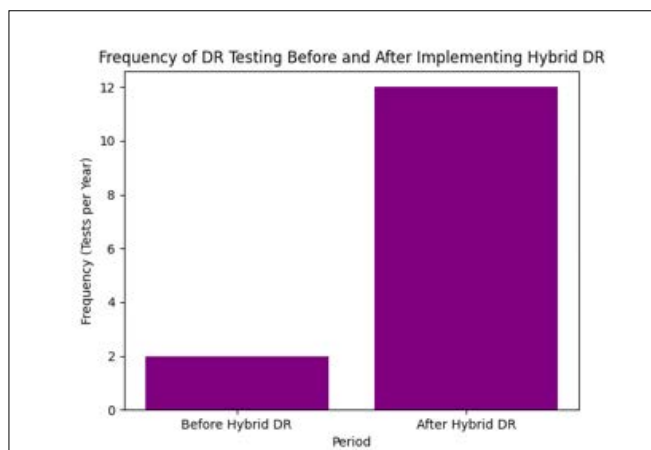
Combining on-premises Hybrid DR design combines HCI with cloud services for scalability and resilience. This step involves designing the hybrid architecture, deploying and configuring components, and testing their compatibility.

The best architectures use cloud and on-premises HCI. Centrally controlled HCI systems incorporate computation, storage, and networking. However, cloud services offer regionally redundant storage and computing capability that may be scaled up or down [11]. The design should include transparent data replication and synchronization between on-premises and cloud settings to ensure data availability and integrity. Hardware, software, and network components (HCI) are assembled and configured for best performance during deployment. Cloud deployments require virtual machines, storage, and networking. Data replication between HCI and cloud environments and flawless failover are crucial setup concerns. Hybrid environment management requires integration and orchestration software. These solutions consolidate on-premises and cloud resource control, automate failover and



failback, and simplify data synchronization. To make DR smooth, all systems and platforms must communicate.

Regular testing and validation make hybrid DR effective. This requires validating failover and failback procedures, periodic DR testing, and DR plan updates and improvements. Tests must be done often to discover and solve issues before they become catastrophic. Simulations of several disaster scenarios are needed to test the DR approach. To be ready, test at least once a year, preferably more often. If a disaster strikes, failover entails shifting operations to the DR site. After a disaster, “failback” permits operations to resume at the original site. Both techniques must be thoroughly tested to ensure compatibility. Checking network settings, software recovery, and data synchronization are included. DR strategies should be revised routinely to reflect testing results, IT landscape changes, and business requirements.



**Figure 5:** Frequency of DR Testing before and after Implementing Hybrid DR

### Best Practices for Implementing Hybrid Disaster Recovery

Hybrid DR works best when tests and practice sessions are done regularly. A lot of DR testing makes sure that people, systems, and processes can work well in a natural disaster. Regular testing keeps the DR plan up to date by showing where it's lacking and where it can be improved. Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) can be met by companies that do DR tests on a regular basis.

These tests check how ready the IT system is and how well the team can carry out the DR plan when things go wrong. Prepare for any problem by practicing different crisis situations [12]. Things that should be covered are natural disasters like floods and earthquakes, cyberattacks like ransomware or DDoS attacks, and technological failures like software bugs. Companies can make a good DR plan by practicing these situations. Hybrid DR plans that work need to be well documented and include training. Stakeholders and staff know what to do in a disaster because they get regular training and the DR plan is well documented. The paperwork for disaster recovery should include backup and failback methods, recovery steps, important staff contact information, and plans for what to do in case of a disaster. This information is very important for everyone on the team to know what to do in an emergency. The staff can learn more about the DR plan and their jobs through regular training and drills. In order to ensure everyone is on the same side; crisis training should cover both technical procedures and communication standards. Getting key people involved in training makes people stronger and more ready. To keep a mixed DR plan in good shape, it needs to be constantly checked on and changed [13]. To keep their DR

plans up to date and ready for action, businesses need to use advanced monitoring tools and keep up with threats and new technology. Monitoring solutions show the state and efficiency of an IT system in real time. When administrators find strange or worrying things, these technologies can let them know about preventative steps. Monitoring operations all the time helps find and fix problems, which cuts down on downtime. As the threats change, new computer threats will appear. These risks must be tracked by businesses, and their emergency recovery plans must be changed as needed. Artificial intelligence (AI) and machine learning (ML) can make DR better in new ways. Adopting this technology makes it easier to plan for, respond to, and predict disasters.

### Future Trends in Disaster Recovery

Due to the fast growth of cloud computing, modern disaster recovery services are easier to get. Because of these improvements, DR systems are now more useful, flexible, and affordable for businesses. Cloud service providers constantly introduce new disaster recovery (DR) options like automatic failover, enhanced data replication, and integrated backup services. Enterprises of all sizes prefer cloud-based DR services because they save time and simplify the process. Machine intelligence is used more in modern DR tactics. These technologies can automate complex processes, speed recovery, and predict errors by analyzing enormous data sets. AI-led DR improves system resilience and recovery. New cyberthreats constantly transform the threat landscape. Companies must modify DR plans to change threats. Smarter ransomware, phishing, and insider threats. Businesses require incident response strategies, behavioral analytics, and threat intelligence to be safe. In addition to cybersecurity, firms must prepare for environmental harm, geopolitical turmoil, and technology issues. Active disaster recovery planning, including risk assessments and scenario planning, prepares organizations for various interruptions. Business disaster recovery is changing with automation and orchestration.

Automating disaster recovery and incorporating DevOps may enhance corporate output and resilience. Automatic data replication, failover start, and system repair are possible with automation. These tools standardize DR processes, speed recovery, and reduce human error. Combining DR with DevOps makes development and release more resilient. This combination makes DR part of software development from testing to deployment and maintenance.

### Conclusion

In conclusion, a hybrid disaster recovery system needs to be tested all the time, have strong security, have a lot of paperwork, and keep getting better. By combining on-premises HCI with cloud services, we can get a reliable, cost-effective, and effective backup option. It's much easier to make changes, add resources, set healing goals, and keep track of everything with hybrid DR. A good and up-to-date DR plan needs to include regular tests and drills, strong security measures, and lots of recordings. If we want to be strong, we need to be able to deal with new tools and risks. Any business worth its salt knows how important it is to have backup plans for when things go wrong. By planning ahead for possible problems, businesses can protect their most valuable assets and cut down on downtime. It is important for everyone to take part and get trained in order to be ready for a disaster. Hybrid DR systems are a smart strategy choice because they are better than traditional methods in many ways. Businesses need to make changes to their emergency recovery plans as threats and technology change. Businesses can keep running smoothly even

when there are problems if they use the newest technology and make plans for how to recover from disasters.

## References

1. N Tabassum, T Alyas, M Hamid, M Saleem, S Malik (2022) Hyper-convergence storage framework for ecocloud correlates. *Computers, Materials & Continua* 70: 1573-1584.
2. H Wen (2019) Improving application performance in the emerging hyper-converged infrastructure," Ph.D. dissertation, Univ. of Minnesota, 2019.
3. P Infrastructure (2020) A paradigm shift towards on-premise modern data center infrastructure for agility and scalability in resource provisioning. *International Journal* 9: 4.
4. S A Azeem, S K Sharma (2017) Study of converged infrastructure & hyper converged infrastructure as future of data centre. *International Journal of Advanced Research in Computer Science* 8: 900-903.
5. S Meneses, E Maya, C Vasquez (2021) Network design defined by software on a hyper-converged infrastructure. Case study: Northern Technical University FICA Data Center," in *Systems and Information Sciences: Proceedings of ICCIS 2020*. Springer International Publishing 272-280.
6. Y Ushakov, M Ushakova, L Legashev (2023) Research of a virtual infrastructure network with hybrid software-defined switching. *Engineering Proceedings* 33: 52.
7. P K Mahapatra, A R Tripathy, A Tripathy (2021) Emerging cloud computing trends for business transformation," in *Machine Learning Approach for Cloud Data Analytics in IoT 2021*: 71-98.
8. B Jadhav, A B Patankar (2019) A novel solution for cloud enabled e-governance using OpenStack: Opportunities and challenges," in *Communication, Networks and Computing: First International Conference, CNC 2018, Gwalior, India, March 22-24, 2018, Revised Selected Papers 1*, Springer Singapore 2019: 24-36.
9. L Militano, A Arteaga, G Toffetti, N Mitton (2023) The cloud-to-edge-to-IoT continuum as an enabler for search and rescue operations. *Future Internet* 15: 55.
10. H Benaddi, N Laaz, A Bouhlal, E Kettani (2023) Data storage architecture for e-government interoperability: Morocco case. *Indonesian Journal of Electrical Engineering and Computer Science* 29: 1678-1686.
11. R J Prabowo, A N Hidayanto, P I Sandhyaduhita, F Azzahro, A Chairunnisa (2018) The determinants of user's intention to adopt hyper-converged infrastructure technologies: An integrated approach," in *2018 International Conference on Information Technology Systems and Innovation (ICITSI)*, IEEE 2018: 306-311.
12. D Mitchell (2017) Introduction to VMware vSAN™ for VMware vCloud Air™ Network," 2017.
13. S Koratagere, R K C Koppal, I M Umesh (2023) Server virtualization in higher educational institutions: a case study. *International Journal of Electrical & Computer Engineering* 13: 4.