Draft Indian Standard

(Draft for comments only)

आपदा रिकवरी - क्लाउड सेवा - दिशानिर्देश

Disaster Recovery - Cloud Service – Guidelines

ICS 35.210

Information Technology and Information Technology enabled Services Sectional Committee, SSD 10

FOREWORD

(*Formal Clauses will be added later*).

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources. Cloud services are designed to provide scalability, flexibility, and cost-effectiveness for businesses and individuals. There has been a significant adoption of cloud technology across user organizations, and a significant upsurge in digital information throughout the user organizations eco-system, hence there is an increased need of preparing our digital ecosystem to overcome any disasters, without a considerable impact on public services.

Cloud disaster services focus on ensuring the availability and resilience of data and applications in the face of unexpected disruptions or disasters. The key components of cloud disaster services include redundancy and high availability, disaster recovery as a service (DRaaS), security compliance, data backup/recovery and testing/simulation. This standard will assist user organizations in evaluating and considering the best practices in terms of disaster recovery and ensuring business continuity.

While preparing this standard, a considerable assistance has been taken from disaster recovery best practices version 1.0, document published by Ministry of Electronics & Information Technology, Government of India.

Draft Indian Standard

DISASTER RECOVERY — CLOUD SERVICE — GUIDELINES

1 SCOPE

This standard provides the guidance to cloud disaster recovery service providers and user organizations (availing cloud disaster recovery service) regarding the strategies and protocols to be adhered to in order to guarantee the availability and uninterrupted provision of their services during a disaster or disruptive incident.

This standard also provides the guidelines for minimizing service interruptions, safeguarding data, and swiftly recovering and reinstating normal operations.

2 REFERENCES

The standards or other publications given below contain provisions which, through reference in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards or other publications are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below:

IS No.	*Title*
IS/ISO/IEC 22123 (Part 1) : 2021	Information technology Cloud computing Part 1: Vocabulary

3 TERMS AND DEFINITIONS

For the purpose of this standard, the terms and definitions given in IS/ISO/IEC 22123 (Part 1) and the following shall apply.

3.1 Application Recovery — A component of disaster recovery that deals with the restoration of business system and data, after the operating system environment has been restored or replaced.

3.2 Business Continuity — A system of planning, for recovering and maintaining both the IT and other functions within a user organizations regardless of the type of interruption. In addition to the IT infrastructure, it covers people, workplaces, facilities, equipment, processes.

3.3 Business Impact Analysis — A collection of information on a wide range of areas from recovery assumptions and critical business processes to interdependencies and critical staff that is then analyzed to assess impact a disaster may have.

3.4 Cloud Service — One or more capabilities offered via cloud computing invoked using a defined interface.

3.5 Cloud Service Provider (CSP) – A party which makes cloud services available.

3.6 Cloud Resources – It encompass a wide range of services and infrastructure components, such as compute resources (virtual machines, containers, functions), storage resources, networking resources, security resources and various application programme interface(s).

3.7 Cold Site — Is a backup location that maintains a replica copy of the production data and configuration with necessary physical space and basic utilities (such as power and cooling) but lacks the IT infrastructure and equipment required for immediate operations. In the event of a disaster, organizations must set up, provision and activate the hardware and software, which can take significant time.

3.8 Disaster Recovery (DR) — Is the process of restoring and maintaining the data, systems, applications and other technical resources on which a business depends.

3.9 Disaster Recovery as a Service — Is the replication and hosting of physical or virtual servers to provide failover in the event of a man-made or natural catastrophe.

3.10 Disaster Recovery Remote Site — It refers to a site that is physically separate from the primary site and provides a secondary instance or replica of IT environment without office infrastructure.

3.11 Disaster Recovery Site (DRS) — It contains the information and applications that are built from the primary repository information. This site is activated whenever the normal site becomes unavailable. The DRS is also known as Secondary Site.

3.12 DR Drill — It is a routine activity done by an organization to check if there is business continuity in case if the Data Centre Site (DC Site) is down due to an unexpected event.

3.13 High Availability — It describes a system's ability to continue processing and functioning for a certain period of time. High availability can be implemented into an organization's IT infrastructure by reducing any single points of failure using redundant components.

3.14 Hot site — Is a fully operational backup location equipped with all necessary hardware, software, and real-time data replication. It ensures minimal downtime in the event of a disaster, allowing for immediate failover to maintain business continuity.

NOTE — Hot sites can be active-active (both sites are live) and active-passive (data is replicated in passive site).

3.15 Infrastructure as a Service (IaaS) — Cloud service category in which the cloud capabilities type provided to the cloud service customer is an infrastructure capabilities type.

3.16 Managed Service Provider (MSP) — Is a third-party company that handles the management and maintenance of cloud infrastructure of user organization.

3.17 Mission-Critical — A computer system or application that is essential to the functioning of business and its processes.

3.18 Normal Site (NS) — Is the site from where the organizations processes and operations are being performed in normal situations. It contains the original data, which is being updated in normal situation. Normal site is also known as Primary site or DC Site.

3.19 Platform as a Service (PaaS) — Cloud service category in which the cloud capabilities type provided to the cloud service customer is a platform capabilities type.

3.20 Recovery Time Objective (RTO) — Is the duration of time and service level within which a business process must be restored after a disruption in order to avoid unacceptable losses. RTO begins when a disaster hits and does not end until all systems are up and running. Meeting tighter RTO, windows requires positioning secondary data so that it can be accessed faster.

3.21 Recovery Point Objective (RPO) — Is the point in time to which an organization must recover data. The RPO is the "acceptable loss" determined by an organization in a disaster situation. The RPO dictates which replication method will be required such as backups, snapshots, continuous replication.

3.22 Software as a Service (SaaS) — Cloud service category in which the cloud capabilities type provided to the cloud service is an application capabilities type.

3.23 Tier 3/3+ compliant — The data center which have multiple paths for power and cooling, and redundant systems that allow the staff to work on the setup without taking it offline. This tier has an expected uptime of 99.982% per year.

3.24 Redundancy — A system of using multiple sources, devices or connections so that no single point of failure will completely stop the flow of information.

3.25 Risk Assessment — The identification and prioritization of potential business risk and disruptions based on severity and likelihood of occurrence.

3.26 Warm Site — Is a backup location that is partially equipped with the necessary hardware and software to support business operations. It typically has some components already provisioned and may include real-time or near-real-time data replication. While it allows for faster recovery than a cold site, it may still require some configuration and additional setup before becoming fully operational site after a disaster. Warm sites strike a balance between cost and recovery speed, making them suitable for organizations with moderate recovery time objectives.

4 UNDERSTANDING OF CLOUD DISASTERS, CAUSES AND TYPES OF DISASTERS

Cloud disasters refer to catastrophic events or situations that impact the availability, performance, or security of cloud computing services. These disasters can lead to significant disruptions in business operations and can have severe consequences for organizations relying on cloud infrastructure and services. Understanding cloud disasters involves recognizing the potential risks, their causes, and implementing strategies to mitigate their impact. The causes and types of disasters are mentioned in Annex A.

5 GENERAL REQUIREMENTS OF CLOUD DISASTER RECOVERY SERVICE PROVIDERS

While considering the services from the cloud disaster recovery service providers, the user organizations should consider the following general requirements:

5.1 Reliability and Availability — The service provider should have a proven track record of high availability and reliability. This includes robust infrastructure, redundant systems, and data centers located in geographically separate seismic zones to ensure data and service availability during a disaster.

5.2 Security — Data security is crucial for disaster recovery. The service provider should have strong security measures in place, including encryption, access controls, distributed denial-of-service (DDoS) protection, firewalls, intrusion detection systems, and regular security audits. Compliance with industry standards and regulations should also be assessed.

5.3 Scalability — The disaster recovery service should be scalable to meet the changing needs of user organization. The provider should offer flexible options to horizontal and vertical scaling of resources as required during disaster recovery scenarios.

5.4 Data Replication and Backup — The service provider should have reliable mechanisms to replicate and backup user organization’s data to ensure its integrity and availability in case of a disaster. This may include features like continuous data replication, incremental backups, point-in-time recovery, and geographically distributed storage. Backup or replication of data can be done in another region or a fully active to active standby can be setup in another region.

5.5 Custom DR Solution — The service provider should have the capability to allow user to deploy third party solution to meet RPO and RTO requirement. The service provider should expose all the services required to build custom solution through API like storage, compute, network, replication etc.

5.6 Recovery Time Objective (RTO) and Recovery Point Objective (RPO) — The service provider should offer solutions/managed services to help organization achieve required RTO and

RPO that align with user organizations recovery goals. Further, the following points should be verified:

a) Applications should be categorized by priority and potential business loss of data in order to focus on defining applications wise RPO and RTO requirement. Applications requiring near zero RTO require failover services;
b) Verify whether application have any service level agreement (SLA) or operation level agreement (OLA) with customers;
c) Individual RPOs typically range from 24h, to 12h, to 8h, to 4h, down to near-zero measured in seconds. Near-zero RPOs will require continuous replication and 4h RPOs will need scheduled snapshot replication;
d) Verify whether application has any dependencies on other application to define RPO; and
e) Verify the RPO dependencies is in terms of the data.

5.7 Testing and Validation — Regular testing (DR dry run) of the disaster recovery solution is essential to ensure its effectiveness. The service provider should support testing processes and provide tools for validating and verifying the recovery process without impacting production systems.

5.8 Monitoring and Reporting — The service provider should have robust monitoring capabilities to track the health and performance of the disaster recovery infrastructure. Real-time alerts and comprehensive reporting should be available to provide visibility into the status of the recovery environment.

5.9 Support and Expertise — The service provider should offer technical support, including assistance during disaster recovery scenarios. They should have knowledgeable staff who understand user organization's requirements and can provide guidance in implementing and managing the disaster recovery solution.

5.10 Cost-effectiveness — Evaluate the pricing structure of the service provider to ensure it aligns with user organization’s budget and offers a cost-effective solution. Consider factors such as pricing models (for example pay-as-you-go or subscription-based), additional charges for data transfer or storage, and any hidden costs.

5.11 Compliance and Regulatory Considerations — If the user organization operates in a regulated industry, ensure that the service provider adheres to the necessary compliance standards and regulations with perspective of business continuity or disaster recovery. While choosing the DRS and replication methodology, user organizations needs to follow the sector-wise guidelines. DR setup/drills should be followed based on sector-wise regulatory requirements. It is recommended that the DC and DR are Tier 3/3+ compliant.

5.12 Location of DC and DR site — The distance for a DR site can vary depending on the types of disaster such as earthquakes, floods, terror attacks, etc. The user organizations should choose a DR

location that fits its business model and regulatory requirements. The DC and DR locations should be ideally in different seismic zones and minimum aerial distance of 100 km. Additionally, the DC and DR site both should not be on the coast of an ocean or same floodplain. Both DC and DR site should be preferably on different regional power grids or different state grids.

5.13 Bandwidth and Latency — Bandwidth and latency are equally critical as other factors while planning DR. User organizations which replicate data for potential failover, both locally and remotely, should take bandwidth requirements into account while planning the DR site. The planning phase of a cloud-based DR implementation involves not only calculations with regard to keeping the offsite data up-to-date and within SLAs, but also with regard to user traffic when an actual recovery is needed. The major considerations while estimating bandwidth requirements while planning a DR site are:

a) While transferring data to the cloud, sufficient bandwidth is required. Hence based on the application and data capacity and criticality, user organizations need to specify the estimated bandwidth requirement;
b) User organizations needs to specify the requirement of redundant network connectivity between DC and DR site;
c) It is necessary to determine the network bandwidth requirements in disaster scenarios, making the data accessible to its users after occurrence of a disaster;
d) The rate of change of data and the frequency of replication are two measure factors which impact bandwidth requirement decisions;
e) Cloud service provider should also have the interconnect/connectivity available between the data centers in different seismic zone; and
f) Cloud service provider should be able to offer bandwidth scalable as per the requirement of the user organization.

5.14 Manpower — The manpower deployed at DRS should have same expertise as normal site to make DRS functional in short notice.

6 DR READINESS AND ASSESSMENT OF USER ORGANIZATION

The assessment of current readiness of user organization regarding DR helps the organization to embark towards the journey of DR. The category of disaster recovery readiness and its result of user organizations are given below in Table 1.

Table 1 Category and Readiness Status of User organizations

(*Clause* 6)

Sl No.	Category	Readiness status	Result
(1)	(2)	(3)	(4)
i)	Category A	No recovery plans	Such user organizations fail to restore operations even during minor outages such as power surge or server crash.

ii)	Category B	Backup of data exist but there are no plans for disaster management	Such user organizations need to back up their data regularly so that they can retrieve their data on the newly replaced systems in case of failure.
iii)	Category C	There is a backup data plan and external site to keep the backed-up data	Such user organizations cannot tolerate to keep their systems down for an extended period. They have an arrangement to restore the required backed-up data which is kept at external site also called as data off-siting.
iv)	Category D	Remote, redundant sites as backup	User organizations which have multiple data centres (at least two) that are located far away from each other. These data centres are interlinked with a strong communication network that facilitates the quick transfer of data in case of any disaster at either of these centres.
v)	Category E	An exact replica of the working data system	This is where the data is backed up almost immediately per hour, per minute or even per second. With this method, user organizations can recover from a disaster almost immediately. Even though this method is the most efficient, it is the most expensive as well.

7 DISASTER RECOVERY PLANNING

The journey towards disaster recovery setup provides step wise guidance in identifying the DR strategy suitable for their respective business. The steps which can be followed while planning for DR is depicted in Fig.1.

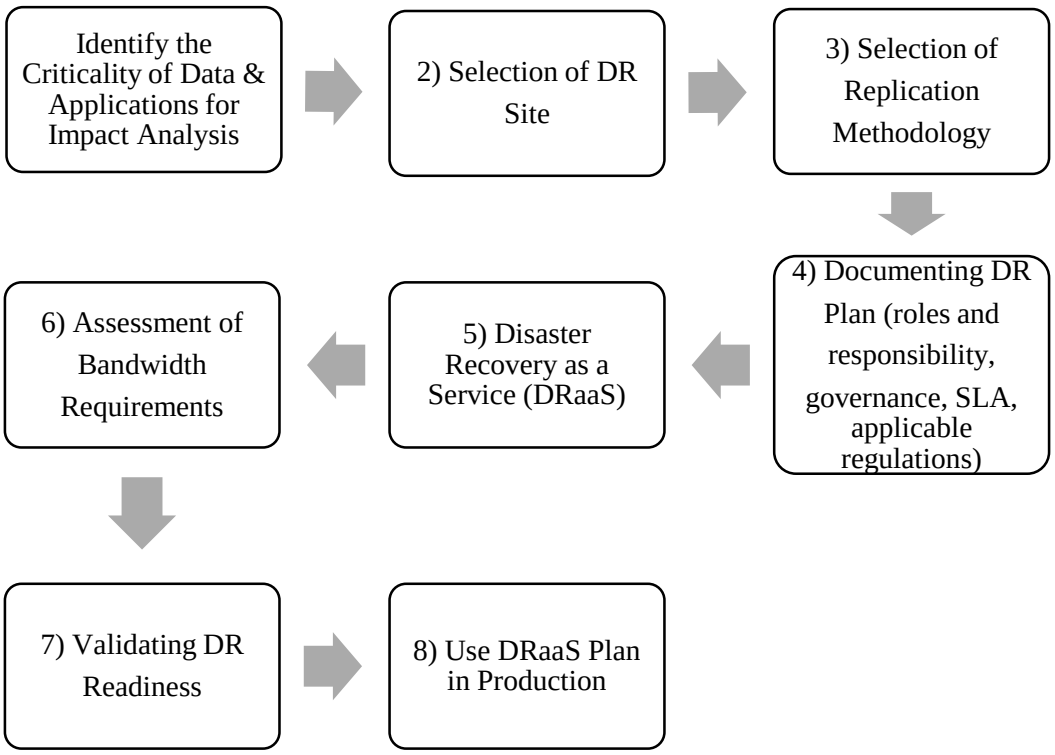

FIG. 1 JOURNEY TOWARDS DR

NOTES

1 For identifying the criticality of data and applications parameters like RTO and RPO should be looked into consideration, see **5.6** for detailed information.

2 DR readiness has to be validated by using application attributes and deployment architectures.

8 IDENTIFICATION OF CRITICALITY OF DATA AND APPLICATION FOR IMPACT ANALYSIS

8.1 Before implementing DR Site, it is important to classify, and group applications based on criticality. Such grouping of applications will help user organizations to distinguish line of applications from each other in terms of their importance to the user organizations, as well as their relative scope of influence on them.

Risk and security assessment framework is recommended to be implemented for impact analysis in the following categories:

a) Assessment of impact on data privacy breach;
b) Assessment of impact on user organizations (tangible), in case of security breach;
c) Assessment of impact on user organizations (intangible), in case of security breach; and
d) Assessment of impact on individual, in case of security breach.

8.2 Based on the impacts (high, medium and low), user organizations can categorize their respective application. For determining the criticality level both the data and applications are important. User organizations should classify application and data based on criticality, as all the data and applications cannot be mission critical.

Low Impact	All data and systems that does not require immediate restoration for the user organization to continue its operations
Moderate Impact	All data and systems that are important user organization can operate but in a diminished state
High Impact	All data and systems without which user organization operation can come to a halt.

8.3 The user organizations data remains equally critical as the data has evolved fast from mere excel or spreadsheet records to representing communication such as e-mail and important digital documents. However, not all data in an enterprise is mission critical. It is important to classify data and define the associated metrics for retention, retrieval and archival. Missing this can increase costs exponentially. Classification helps in narrowing down the actual data that needs to be recovered in the case of a disaster.

8.4 Categorizing business requirements based on priorities should be finalized. The below classifications will detail out the baseline for decision-making matrix.

Criticality Level	*Implications*
Mission Critical data/applications	a) Widespread stoppage of applications with significant impact on User organizations operations. b) Public, wide-spread damage to user organizations reputation
Essential data/applications	a) Direct impact on operations b) Direct negative user satisfaction c) Compliance violation d) Non-public damage to user organizations reputation
Core data/applications	a) Indirect impact on operations b) Indirect negative user satisfaction c) Significant user organizations productivity degradation
Supporting data/application	a) Moderate User organizations productivity degradation

9 SELECTION OF DR SITE

Based on the criticality of applications and data, user organizations need to determine the best suited DR site for their disaster recovery planning and business continuity strategies. The user organization depending on the organization's specific needs, budget, and acceptable downtime may choose hot site, warm site or cold site as DR site. The deployment architecture of DR strategies are given in Annex-C. The characteristics of these three sites are given below:

Characteristics	*Hot Site*	*Warm Site*	*Cold Site*
Cost and recovery time	Hot sites are the most expensive and offer the shortest recovery time.	Warm sites are moderate cost and Recovery time is faster than a cold site but slower than a hot site.	Cold sites are cost-effective but involve longer recovery times.
Application	Used for business critical application	Used for no business critical application	Used for no business critical application
Disaster readiness	Ready in the event of disaster	Data is replicated but servers may not be ready	Not ready for automatic failover
Data Risk	None	Low	High
Infrastructure	Full	Moderate	Minimal

10 SELECTION OF REPLICATION TECHNOLOGY

10.1 Identification of Replication Technology

Data replication is a way to ensure that user organizations are prepared for disasters. Replication creates copies of data at varying frequencies, depending on the data in question and the industry of the organization backing it up. In the event of a disaster, the primary systems failover to this replicated system. The two types of data replications are synchronous and asynchronous replication.

10.1.1 *Synchronous Replication* — In synchronous replication, the copies of data are created in real time on secondary site and locally. Further, it ensures the following:

a) Business continuity,
b) Very low RTO/RPO,

c) DC and DR sites are in close proximity, and
d) Minimize downtimes and assure a high infrastructural availability.

In synchronous replication the two sites cannot be far from each other and is an expensive methodology.

10.1.2 *Asynchronous Replication* — In asynchronous replication, the copies of data are created as per defined schedule and is suitable for user organizations that can endure longer RTOs. In this replication, the DC and DR sites are distant apart, and it allows to protect business even in case of large-scale disasters which may damage both sites (for instance, an earthquake).

10.2 The replication methodologies can also be controller based. Some of the methodologies in controller-based replication are mentioned below:

Parameter	*Array Based*	*Application Based*	*Host Based*	*Network Based*
Support of Heterogeneous Application	Low and works for similar arrays	Low and works for specific application only	High storage agnostics	High storage array and platform agnostics
Performance and Scalability	Good in high end arrays	Good for single application platform	Workload is spread across servers	Good
Cost	High entry cost	High entry cost	Low entry cost and cost is based on number of servers	High end entry cost and requires intelligent switches
Replication Modes	Synchronous and asynchronous	Synchronous and asynchronous	Asynchronous	Synchronous and asynchronous

10.3 Data Replication

Data replication is a critical aspect of resiliency in cloud computing because it ensures that data is available even in the event of a failure. Replication involves creating copies of data and storing them in multiple locations, which can be used to recover from a failure or disaster. Appropriate storage option for data replication should be selected. The types of storage options for replicating data is given in Annex-D.

11 DOCUMENTATION OF DR PLAN

11.1 While documenting DR plan, user organizations should take a holistic view and focus on recovering the application services and not just servers. The technical recovery plan for each application/service should be documented in a way that all the activities that need to be performed during recovery should be defined in a sequential manner. The user organization should also

a) Design for end to end recovery;
b) Define recovery goals;
c) Make tasks specific to make the system up and running;
d) Ensure compliance with its own laws and regulations, as well as any applicable external legal requirements and guidelines, including contractual obligations and regulatory authorities;
e) Document all the steps that is needed; and
f) Maintain more than one DR recovery paths.

Further, it should cover all details such as physical and logical architecture, dependencies (inter and intra-application), interface mapping, authentication. Application dependency matrix, interface diagrams. Application to physical/virtual server mapping play an important role in defining how applications interact with each other to deliver various functionalities.

11.2 The roles and responsibilities should be clearly defined while planning for a DR Site. It should contain a governance and reporting structure often in the form of a business continuity committee. The committee will ensure senior management commitments and define senior management roles and their respective responsibilities. The business continuity committee should include the following members:

a) Disaster recovery planning (DRP) coordinator from user organization — The DRP coordinator shall have comprehensive decision-making powers, member from the higher authority expected to lead the DR activities

b) Disaster recovery service (DRS) coordinator from service provider — The DRS coordinator will be single point contact for providing DR service from the service provider and will act as per direction from DRP coordinator.

c) Crisis management team (CMT) — The CMT shall comprise of management level personnel who shall analyze the damage at DC, advise the DRP coordinator for disaster declaration, and initiate the recovery of operations at the DR Site.

d) Third party services coordinators from the third-party services provider organizations — There can be multiple third-party services in cloud and for a complete disaster recovery it is needed to identify third party services coordinators who will act as per DRP coordinator and CMT.

e) Damage assessment team (DAT) — The damage assessment team shall comprise of a management and technical expertise mixture of personnel who shall assess and report the damage at DC and take steps to minimize the extent of the same.

f) Operations recovery team (ORT) — The operations recovery team shall comprise of a management and technical expertise mixture of personnel who shall undertake the recovery operations at the designate DR Site.

11.2.1 *Roles and Responsibilities of Business Continuity Committee*

The roles and responsibilities of business continuity committee are given below:

a) Clarifying their roles of all the members of the committee,
b) Oversee the creation of a list of appropriate committees, working groups and teams to develop and execute the plan,
c) Provide strategic direction and communicate essential messages,
d) Approve the results of business impact analysis,
e) Review the critical services and products that have been identified,
f) Approve the continuity plans and arrangement,
g) Monitor quality assurance activities,
h) Resolve conflicting interests and priorities.

11.3 Segregation of Responsibility Between CSP, MSP and a User Organizations

The segregation of responsibility between CSP, MSP and a user organization is given in Annex B.

11.4 Scope and Dependencies

Identifying key cloud resources and incorporating them into the recovery scope can contribute to achieving shorter recovery time objectives. These resources should host business-critical data and applications. Additionally, it is essential to consider the dependency relationships between these cloud resources, applications, and IT systems. For instance, the functionality of a specific application may rely on data stored in another cloud resource, or vice versa. Dependencies also extend to employees and infrastructure components. Understanding and documenting these dependencies is crucial to ensure that user organizations can maintain operations with minimal disruption..

11.5 Service Level Agreement

Service Level Agreement (SLA) as already detailed out in **5** can be referred for key parameters on which SLAs to be negotiated, while finalizing the cloud disaster service recovery offerings.

12 IMPLEMENTATION AND CONSIDERATIONS FOR DISASTER RECOVERY AS A SERVICE (DRAAS)

12.1 It is expensive to maintain a dedicated DR site, user organizations can choose to outsource this cost. Replacing the cost of dedicated site with a predictable expense is comparatively better option. DRaaS enables full replication and backup of all cloud data and applications while serving as a secondary infrastructure. It actually becomes the new environment and allows an organization and

users to continue with daily operations while the primary system undergoes restoration. The following are the reasons to consider DRaaS over on-premise DR Site:

12.1.1 *On-demand Provisioning* — All cloud services offer on-demand self-service functionality. Once the service is initiated by the user, it takes only few minutes to get commissioned, which is much faster than commissioning the same service on premise.

12.1.2 *Easy Scalability* — Cloud services can be scaled exponentially. Adding resources to a cloud-based solution takes very less time and effort. On the other hand, if on premise DR is present, then user organizations should be sure about the capacity in order to provide an adequate DR coverage.

12.1.3 *Removes Maintenance Overhead* — As cloud platforms are part of managed service, maintaining and upgrading the underlying infrastructure is the responsibility of the cloud service provider. If internal DR environment is present with the user organizations, it also needs to be upgraded with the new features and patches, which require overhead of IT resource.

12.1.4 *DRaaS is Cost Effective* — Cloud services works on pay per use model which is extremely cost effective as user organizations can diligently control their spending by consuming and only paying for the resources they use. In case of on-premise environment, resources are often underutilized and do not run at full capacity. Enough hardware procurement is also an overhead cost.

12.1.5 *Multisite* — Resources can be replicated to many different sites to ensure continuous backup in the event of unavailability of one or more sites.

12.1.6 *Service Provider Agnostic* — DRaaS replicates any environment and is not service provider specific.

12.2 Disaster Recovery Management Tool

A disaster recovery management tool is a component of a Disaster Recovery as a Service (DRaaS) solution. It assists user organizations in maintaining or swiftly restoring their mission-critical functions following a disaster. This tool supports preventative planning and execution for catastrophic events that could severely impact computers, servers, or networks. It enables an organization to operate instances of its applications in the cloud service provider's (CSP) environment. A key advantage is the significant reduction in the time required to return applications to production, provided networking issues are resolved, as there is no need to restore data over the Internet.

12.3 Factors Affecting DRaaS Pricing

DRaaS is often made up of several pricing components, including:

a) Replicated data storage cost
b) Software licensing costs (for disaster recovery and business continuity software to provide data replication)
c) Computing infrastructure cost
d) Bandwidth cost

e) SLA based cost

NOTE — Some DRaaS providers only charge for storage and software licensing when the service is not actually being used, adding compute infrastructure and bandwidth costs if the service is activated in the case of a disaster. Others charge for all components in the form of a "service availability fee," regardless of whether or not the service is actually used.

13 ASSESSMENT OF BANDWIDTH AND LATENCY REQUIREMENTS

The assessment of bandwidth and latency requirements are mentioned in **5.1.13**.

14 VALIDATION OF DR PLAN

The readiness assessment will help in evaluating the current status of disaster recovery. Whenever downtime happens, for any reason, data/applications become unavailable to the users, which leads to an abrupt halt of all the functions.

The replicated resources to be reviewed at least twice in a year based on sector wise requirements, to ensure resources are effectively replicated and identified resources are in alignment with the business priorities and goals.

14.1 Elements for Validation of DR Plan

The following elements should be ensured while validation of DR plan:

a) DR Drill;
b) Business impact analysis and risk assessment;
c) Application dependencies and interdependencies;
d) Recovery time objectives (RTO);
e) Recovery point objectives (RPO);
f) Backup procedure defined in **D-2** should be validated; andIT and senior management signoff.
    1) Based on end-to-end DR solution, identify and engage all resources needed to support DR test (process owners, system owners, customer, suppliers)
        i) List teams and tasks of each
        ii) Obtain emergency resources such as set up transportation to and from backup site, if necessary
        iii) List all personnel and their telephone numbers
        iv) Establish user participation plan
    2) Define DR test approach and seek approval
    3) Define test activities (DR end-to-end test plan)
    4) Verify the network infra dependencies
        i) Check out any off-line equipment needs for each application
    5) Verify network firewall device changes at DC and DR locations
    6) Verify the operating system dependencies
    7) Determine applications to be run and in what sequence

8) List out the services required at DR end
9) Check all data being taken to backup site before leaving and leave inventory profile at home location
10) Define roll-back plan and estimate timings.
11) Contact vendors both hardware and software
12) Notify users of the disruption of service
13) Storage for essential records

14.2 Execution of DR Plan

While execution of DR plan the following should be ensured:

a) Stop all the Services at DC and verify DR site is in sync and active;
b) Disable replication;
c) Shutdown all applications at DC;
d) Stop the Database;
e) Confirm shutdown procedure at DC; and
f) Verify the logs.

a) During failover to DR
   1) Verify the Network Infra;
   2) Verify network firewall device status at DR location;
   3) Verify Connectivity of the operating system;
   4) Validate isolation of DR site from primary;
   5) Verify receipt of database transaction;
   6) Start all standard jobs; and
   7) Functional health check.

b) During failback to DC
   1) Verify network firewall device configuration at DC location;
   2) Verify the operating system dependencies;
   3) Start the services required at DC Location;
   4) Verify whether application and database replication working fine; and
   5) Restart the jobs.

14.3 Evaluation of DR drill outcome/results

The outcomes/results of evaluation of DR drill are:

a) Review of the test results against the POA;

b) Verify the RTO and RPO target values vs achieved values;

c) Sign-off from the customer; and

d) Areas of improvement with ownership and proper corrective action plan if the RTO and RPO is not achieved properly.

15 USING DRAAS PLAN IN PRODUCTION

15.1 Operation from the DR Site

In case of failure of primary site when the service is running from the DR site efforts may be made to restore the primary site within a reasonable time. In case of any delay in restoration necessary provisions such as backup, monitoring at the DR site should also be implemented.

ANNEX A
(*Clause 4*)
(Informative)

CAUSES AND TYPES OF CLOUD DISASTERS

Cloud disasters can pose significant threats to the seamless functioning of cloud services. Understanding the causes and types of cloud disasters is crucial for organizations to implement robust disaster recovery plans.

A-1 CAUSES OF CLOUD DISASTERS

A disaster can be related to any incident (both intentional and/or non-intentional) that causes severe damage to the operations and data of any organization.

A-2 TYPES OF CLOUD RELATED DISASTERS

The following are the primary categories of cloud-related disasters:

a) Natural Disasters — Events like earthquakes, hurricanes, floods, or wildfires can damage data centers or network infrastructure, leading to service outages or data loss.

b) Hardware or Software Failures — Malfunctioning hardware components, software bugs, or compatibility issues can cause service disruptions or data corruption.

c) Cyber security Breaches — Security vulnerabilities, hacking attempts, ransom ware attacks, or malware infections can compromise cloud systems, leading to unauthorized access, data breaches, or service interruptions.

d) Human Errors/Man Made Errors — Misconfiguration, accidental deletions, or improper maintenance can cause data loss, service interruptions, or security breaches.

e) Power or Network Failures — Power outages, network failures, or inadequate redundancy measures can impact the availability and reliability of cloud services.

ANNEX B

(*Clause* 11.3)

(Normative)

RESPONSIBILITY BETWEEN CSP, MSP AND A USER ORGANIZATIONS

B-1 The segregation of roles and responsibilities between a user organization, MSP and CSP is depicted in the Table 2.

Table 2 Responsibility between CSP, MSP and User organization

(*Clause* B-1)

Sl No. (1)	**Responsibility** (2)	**Disaster Recovery Management** (3)	**SaaS** (4)	**Paas** (5)	**IaaS** (6)	**On-premise** (7)
i)	Responsibility Always Retained by the User organization /MSP	Information and Data	User organization/ MSP	User organization /MSP	User organization /MSP	User organization/ MSP
		Devices (Mobiles and PCs)	User organization/ MSP	User organization /MSP	User organization /MSP	User organization/ MSP
		Accounts and Identities	User organization/ MSP	User organization /MSP	User organization /MSP	User organization/ MSP
ii)	Responsibility Varies by Type	Identity and Directory Structure	CSP (C,I)	CSP (C,I)	CSP (C,I)	User organization/ MSP (R,A)
			User organization/ MSP (R,A)	User organization /MSP (R,A)	User organization /MSP (R,A)	
		Applications	CSP (R,A)	CSP (C,I)	CSP (C,I)	User organization/ MSP (R,A)
			User organization/ MSP (C,I)	User organization /MSP (R,A)	User organization /MSP (R,A)	
		Network Controls	CSP (R,A)	CSP (C,I)	CSP (C,I)	User organization/ MSP (R,A)
				User organization /MSP	User organization /MSP	

				(R,A)	(R,A)	
		Operating System	CSP (R,A)	CSP (R,A)	CSP (R,A)	User organization/ MSP (R,A)
			User organization/ MSP (C,I)	User organization /MSP (C,I)	User organization /MSP (C,I)	
iii)	Responsibility transfers to CSP	Physical Hosts	CSP (R,A)	CSP (R,A)	CSP (R,A)	User organization/ MSP (R,A)
		Physical Network	CSP (R,A)	CSP (R,A)	CSP (R,A)	User organization/ MSP (R,A)
		Physical Data Centre	CSP (R,A)	CSP (R,A)	CSP (R,A)	User organization/ MSP (R,A)
iv)	Responsibility of DR Drill	Preparation of DR Test Plan	CSP (R,A)	CSP (C,I)	CSP (C,I)	User organization/ MSP (R,A)
				User organization /MSP (R,A)	User organization /MSP (R,A)	
		Review and approval	User organization/ MSP (R,A)	User organization /MSP (R,A)	User organization /MSP (R,A)	User organization/ MSP (R,A)
		Execution of DR Plan	CSP (R,A)	CSP (C,I)	CSP (C,I)	User organization/ MSP (R,A)
				User organization /MSP (R,A)	User organization /MSP (R,A)	
		Verify the Test Results	CSP (R,A)	CSP (C,I)	CSP (C,I)	User organization/ MSP (R,A)
			User organization/ MSP (C,I)	User organization /MSP (R,A)	User organization /MSP (R,A)	

		Evaluation of DR	CSP (R,A)	CSP (C,I)	CSP (C,I)	User organization/ MSP (R,A)
			User organization/ MSP (C,I)	User organization /MSP (R,A)	User organization /MSP (R,A)	
		Proper Corrective Action Plan if the RTO is achieved properly.	CSP (R,A)	CSP (R,A)	CSP (R,A)	User organization/ MSP (R,A)
			User organization/ MSP (C,I)	User organization /MSP (C,I)	User organization /MSP (C,I)	
		Proper Corrective Action Plan if the RPO is achieved properly	CSP (R,A)	CSP (C,I)	CSP (C,I)	User organization/ MSP (R,A)
			User organization/ MSP (C,I)	User organization /MSP (R,A)	User organization /MSP (R,A)	
		DR Test Report	CSP (R,A)	CSP (C,I)	CSP (C,I)	User organization/ MSP (R,A)
				User organization /MSP (R,A)	User organization /MSP (R,A)	
A – Accountability, R – Responsibility, I – Information, C - Consulted NOTE — In case of execution of DR plan (SaaS) user organization/MSP will be informed.						

ANNEX C
(*Clause* 9)
(Informative)
DEPLOYMENT ARCHITECTURE OF DR STRATEGIES

The different deployment architectures that fall under the two broad DR strategies (RPO and RTO) are given below:

Strategy	*Deployment architecture*	*RPO*	*RTO*
Active/standby	Cold standby	Hours	Hours
Active/standby	Warm standby	Seconds	Hours
Active/standby	Hot standby	Seconds	Minutes
Active/active	Active/active	Near zero	Near zero

C-1 DC Requirements for Different Deployment Architecture

The following describes the data centre requirement and suitable mitigation scenarios based on the different deployment architecture:

Deployment architecture	*Data centre requirement*	*Suitable mitigation scenarios*
Cold standby	Require local backup copies in same DC on different storage type and also backup copies in different DC.	Human cause events like human errors (like data deletion or data corruption), Malicious attacks from outside and inside.
Warm standby	Require multiple DC in different seismic zones or at least 100km away from each other.	Natural Disasters like Flood, Earth Quake, Storm, Terrorist attack, Political reasons. This deployment can also handle operational failures with higher RPO and RTO.
Hot standby and Active/active	Require multiple DC within a short distance or within same city	Operational failures like Power failure, IT hardware failure, Network failure, IT software failure.

C-2 Cloud Based Deployment Architectures

Cloud based deployment architecture describes how various components such as compute, platform/database, and applications are deployed between cloud regions to create a resilient means

of recovering from the total failure of a data center. This architecture describes where everything is located during the normal operation of an application suite and what needs to be recovered at the standby region to get things running again. The following should be considered by the CSP:

a) CSP should offer their customers the freedom to choose "all of the above" solutions to meet SLAs for the wide variety of business systems that organizations typically support.

Many terms are used to describe DR strategies and deployment architectures. However, the various approaches and patterns for describing how to deploy the infrastructure, platform, and applications for disaster recovery fall into two broad strategic categories: active/active and active/standby DR.

C-2.1 *Active/Active Deployment Architecture*

In active/active deployment architecture, the entire application stack is fully functional and handles a workload at both the primary and standby regions. For databases, respective native replication and active/active technologies will be used to keep the database synchronized between primary and standby regions. Applications are running and accessible over the public-facing network at the standby cloud region and have a running workload. The Fig. 2 demonstrates the active/active deployment architecture.

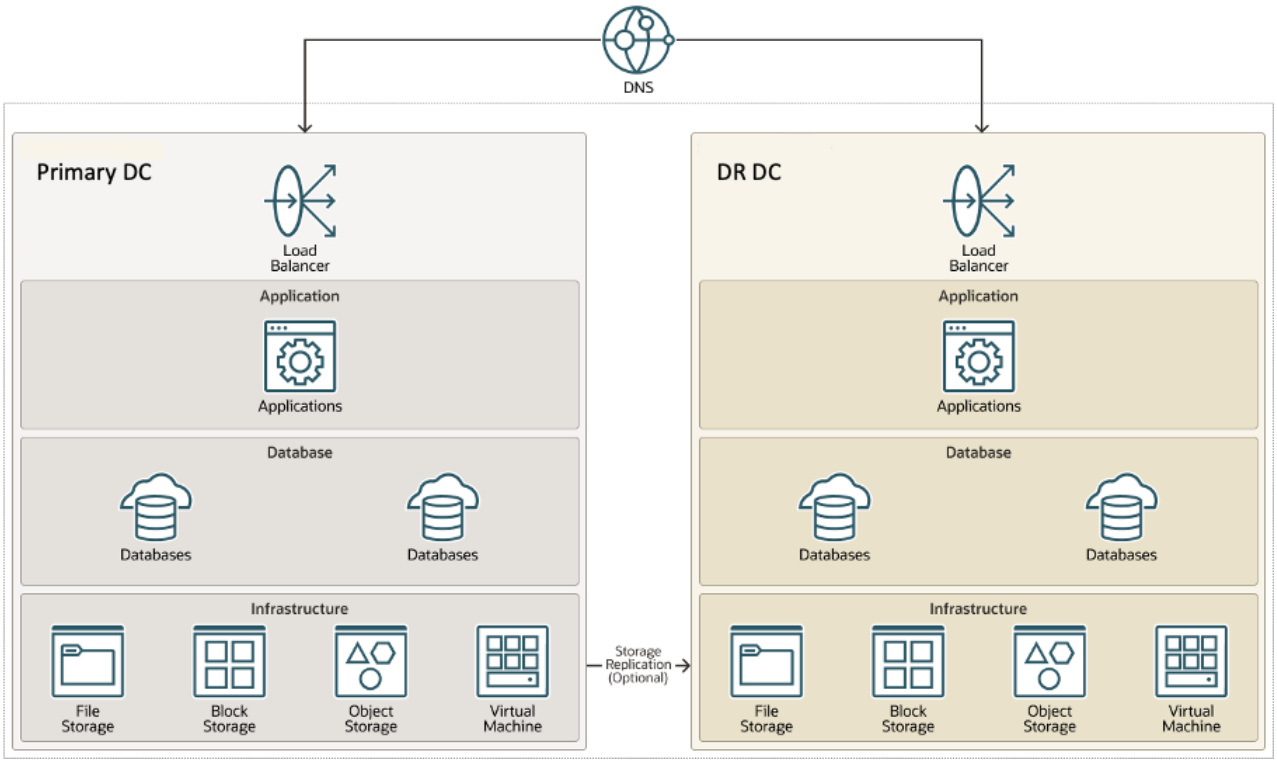

FIG. 2 ACTIVE/ACTIVE DEPLOYMENT ARCHITECTURE

C-2.2 *Active/Standby Deployment Architectures*

There are many variations of active/standby deployment architectures. Active/standby deployments, sometimes called active/passive deployments, are often characterized as cold, warm, and hot standby deployments.

Cold standby, Warm standby, and Hot standby scenarios all represent some form of the same theme where 100% of an application stack is running at the primary region while 100% or less than 100% of the same business system is actively running in the standby region.

The following series of very high-level conceptual diagrams is meant to illustrate some fundamental differences between common deployment architectures and are not meant as reference architectures; they do not describe how to implement DR for an application stack. Refer to Fig. 2 for active/standby architecture

C-2.2.1 *Cold standby site deployment architecture*

In cold standby scenario, the virtual machines (VMs), database, and applications only exist at the current primary region. The file and block storage volume groups containing the boot disk and any other virtual disks for each VM are replicated to the standby region. Fig. 3 demonstrates cold standby architecture.

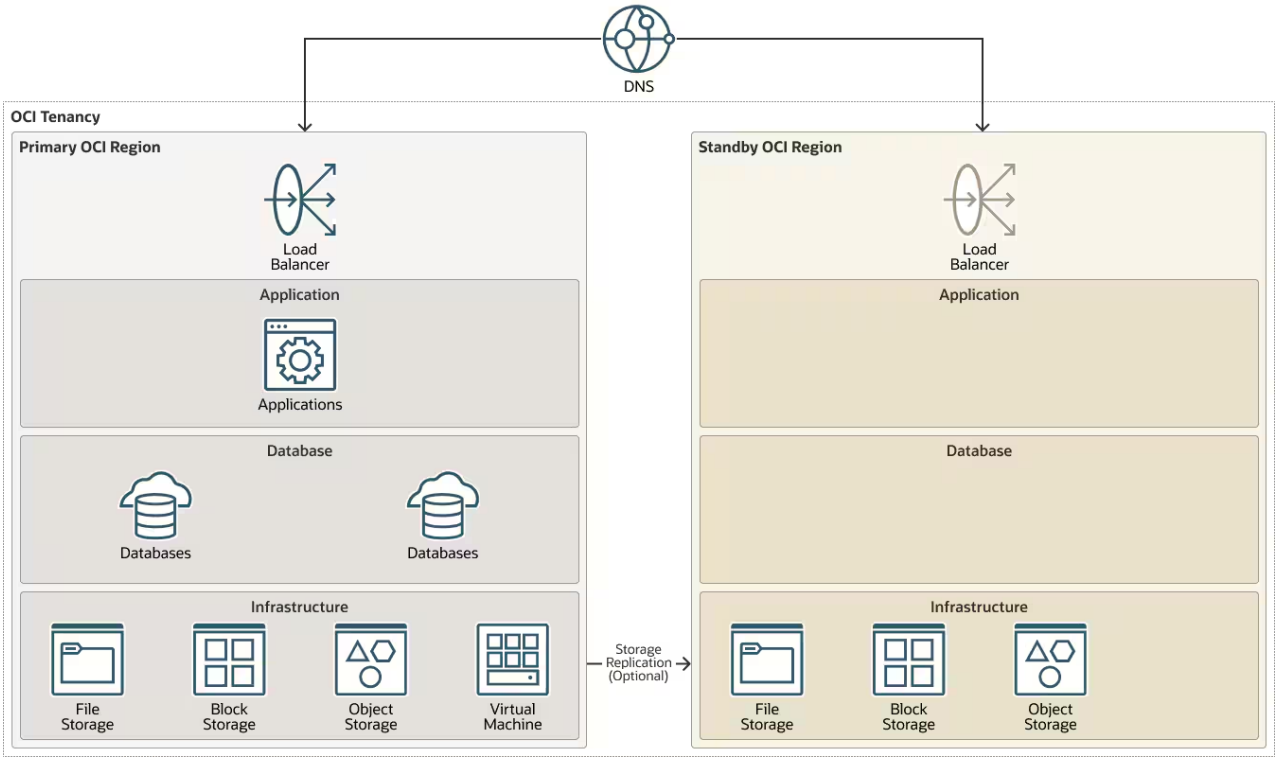

FIG. 3 COLD STANDBY SITE DEPLOYMENT ARCHITECTURE

During a DR operation such as a switchover or failover, the replicated storage containing the same VMs is activated at the standby region, and the same exact VMs are started again at the point where

they were stopped or crashed. The VMs are the same exact virtual machines that were formerly running at the active region.

This deployment architecture has several advantages, including lower deployment costs, lower maintenance overhead, and lower operating costs.

C-2.2.2 *Warm standby site deployment architecture*

In this scenario, virtual machines exist at both the primary and standby regions but are completely independent of each other and have their own unique host names and preassigned IP addresses. The VMs at the standby region exist and can be stopped or running depending on customer preference. Fig. 4 demonstrates warm standby architecture.

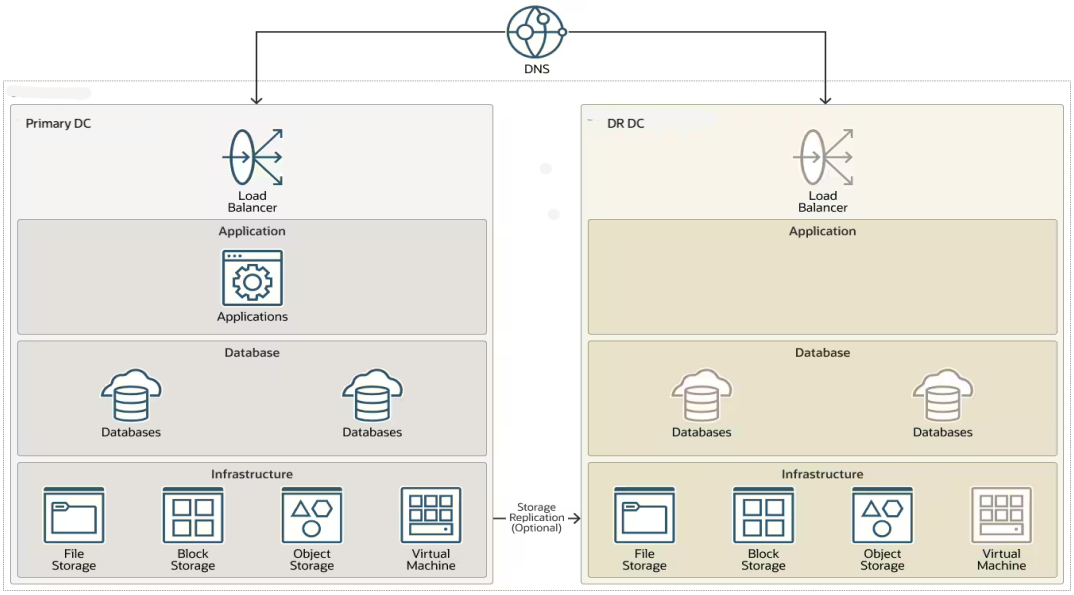

FIG. 4 WARM STANDBY SITE DEPLOYMENT ARCHITECTURE

C-2.2.3 *Hot standby site deployment architecture*

In this scenario, virtual machines exist and are running at both the primary and standby regions with their own unique host names and preassigned IP address. Databases should be running at both the primary and standby regions. Applications are running at the standby cloud region, but are not accessible over the public-facing network. Fig. 5 demonstrates hot standby site deployment architecture.

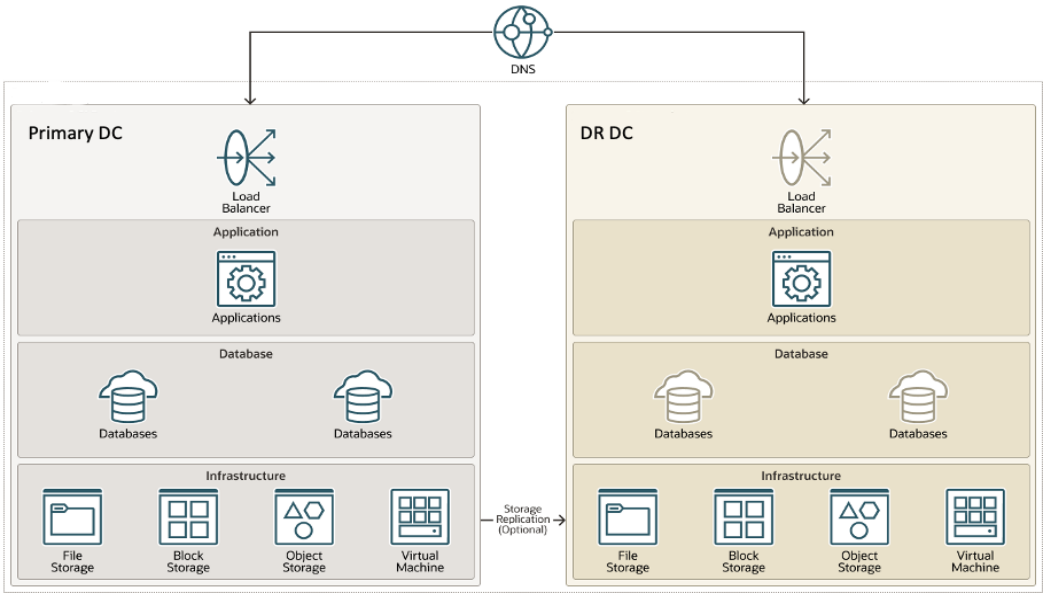

FIG. 5 HOT STANDBY SITE DEPLOYMENT ARCHITECTURE

ANNEX D
(*Clause* 10.3)
(Informative)
TYPES OF STORAGE OPTIONS FOR REPLICATING DATA

D-1 The types of storage options for replicating data are given below:

a) *Object Storage* — is a highly scalable and durable storage service that enables replication of data across regions. By configuring cross-region replication, data is automatically replicated to a different region, providing a high level of resiliency. In the event of a disaster or outage, data can be easily accessed from the replicated location, ensuring business continuity.
b) *File Storage* — provides highly available and durable file systems that can be accessed by multiple instances simultaneously. By using Replication Policies, files can be replicated to maintain multiple copies within DC and to DR data center, providing fault tolerance and high availability.
c) *Block Volume Level Storage Replication* — can be used keep multiple copies of block volume within the primary data centre and on the DR data centre. This ensures that data is available even in the event of a failure or outage.

Data replication is crucial for maintaining resiliency in cloud computing, and CSP provides several options to replicate data across regions, within primary datacentre (region), and instances. These options, can be used to ensure that your data is highly available, durable, and easily recoverable in the event of a failure or disaster.

D-2 The Design of Data Backup Strategy

The data backup strategy should be well defined which includes the following:

a) The data backup procedure should include full, incremental, differential backup strategies which are aligned as per the required RTO and RPO,
b) Offsite storage for essential records, and
c) Data retention policies.