DR Solutions Design and Review

Activity 1: DR Terms and Concepts

Read Abualkishik et al. (2020) and answer the following questions:

1. What is the difference between Hot Standby, Warm Standby and Cold Standby? Frame your answers in terms of availability, RPO and RTO.
2. Does the technology deployed affect the options available? For example, can you create a high availability, hot standby solution between two on-premise data centres?

RTO - Recovery Time Objective

RPO - Recovery Point Objective

Hot Standby

Availability: High. Systems are fully operational and ready to take over immediately.

RTO Very Low (minutes or seconds). Failover is almost instantaneous.

RPO Very Low (near-zero). Data is synchronised in real-time or near real-time.

Deployment: Requires advanced clustering, real-time replication and monitoring.

Technology Consideration: It can be built between two on-premises data centres, but it requires high-speed connectivity, synchronous replication and robust failover mechanisms e.g. VMware. It is costly and technically complex but feasible.

Warm Standby

Availability: Moderate. Systems are pre-configured but not actively running.

RTO: Moderate (hours). Systems need to be started, services redirected.

RPO: Moderate (hours). Data may be replicated periodically or in batches.

Deployment: Involves maintaining idle but ready to activate infrastructure.

Technology Consideration: Easier to implement than hot standby. Suitable for both cloud and on-premises setups. Less demanding on bandwidth and system integration.

Cold Standby

Availability: Low. Only infrastructure is in place, system setup begins after a disaster.

RTO: High (days). Time needed to install software, restore data, configure systems.

RPO: High (days or last backup). May involve significant data loss if backups are not recent.

Deployment: Simple and cheap, but recovery is slow.

Technology Consideration: Can be done on-premises or in the cloud. Suits non-critical systems.

Type	Availability	RTO	RPO	Typical Use Case
Hot	High	Minutes	Near Zero	Critical services requiring zero downtime
Warm	Medium	Hours	Hours	Important services with some tolerance
Cold	Low	Days	Days	Non-critical systems, cost saving

Activity 2: DR Solutions Design

Read Morrow et al. (2021) and answer the following questions:

1. What are some of the main vendor lock-in issues the authors identify? How would you mitigate them?
2. What are some of the security concerns with the modern cloud? How can these be mitigated?

Cloud Service Provider (CSP): Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP).

Vendor Lock-In Issues Identified

- **Unique CSP Architectures:** Each cloud provider uses proprietary services, APIs and infrastructure. Migration to another CSP can require major redesign efforts.
- **Asymmetric Data Transfer Costs:** It is often cheap to upload data to a cloud, but expensive to extract it, creating a financial barrier to exit.
- **Data Portability in SaaS:** SaaS platforms often do not offer standardised tools for exporting data, making it hard to migrate or back up independently.
- **Employee Expertise:** Teams become highly specialised in one CSP's ecosystem.
- **Use of Proprietary Features:** Taking advantage of CSP-unique capabilities.

Mitigations for Vendor Lock-In

- **Plan for Decommissioning Early:** Include exit strategies in the initial deployment plan.
- **Choose Standardised Services**: Prioritise open-source or cross-cloud tools over proprietary ones.
- **Regularly Export Data:** Validate that data can be extracted in a usable format.
- **Maintain Skills Flexibility:** Encourage cross training across platforms.

Modern Cloud Security Concerns

- **Misconfigurations:** Especially in storage services.
- **Credential Compromise:** Often via weak or single-factor authentication, insider threats and overprivileged accounts.
- **Inadequate Monitoring:** Delayed detection of breaches.
- **Supply Chain Risks:** Attackers exploiting third-party software or tools (SolarWinds).

Mitigations

- **Multi-Factor Authentication (MFA):** Especially for privileged accounts.
- **Zero Trust Architecture:** Always verify identity and permissions.
- **Encrypt Data at Rest and in Transit:** Use CSP or third-party key management tools (KMS).
- **Define and Enforce Access Policies:** Apply least privilege and regular audits.
- **Comprehensive Monitoring:**
  - Leverage CSP tools like AWS CloudTrail, Azure Sentinel.
  - Integrate cloud and on-premises logs for full visibility.
- **Regular Security Reviews:** Especially when services or architectures change.
- **Backup Critical Data Off-CSP:** To maintain availability and recovery options.

Activity 3: DR Solutions Design and Review

Create a high-level diagram of a DR solution for each of the following requirements. They should be created in PowerPoint, and you should include a basic description of each design.

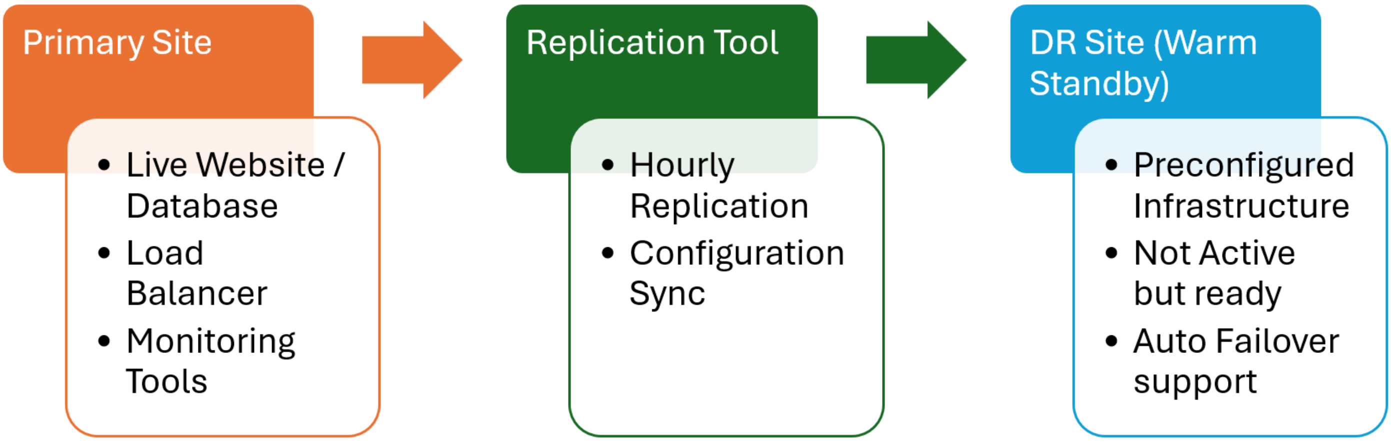
RPO= 1 hr; RTO= 8 hrs; high availability (HA) required.
RPO= 24 hrs; RTO = 72 hrs; HA NOT required.
RPO= 5 mins; RTO= 1 hr; HA required.

Scenario 1: RPO = 1 Hour; RTO = 8 Hours; High Availability Required

This scenario is ideal for systems that are highly available and customer-facing, where some brief data loss is acceptable, but service continuity is essential. Systems are designed for automated failover with warm standby infrastructure and data is replicated hourly.

Typical Applications:

- Customer-facing websites and portals
- Order management or e-commerce frontends
- CRM systems with external integrations
- Customer support tools or service desks



Primary Site

- Live Website / Database
- Load Balancer
- Monitoring Tools

Replication Tool

- Hourly Replication
- Configuration Sync

DR Site (Warm Standby)

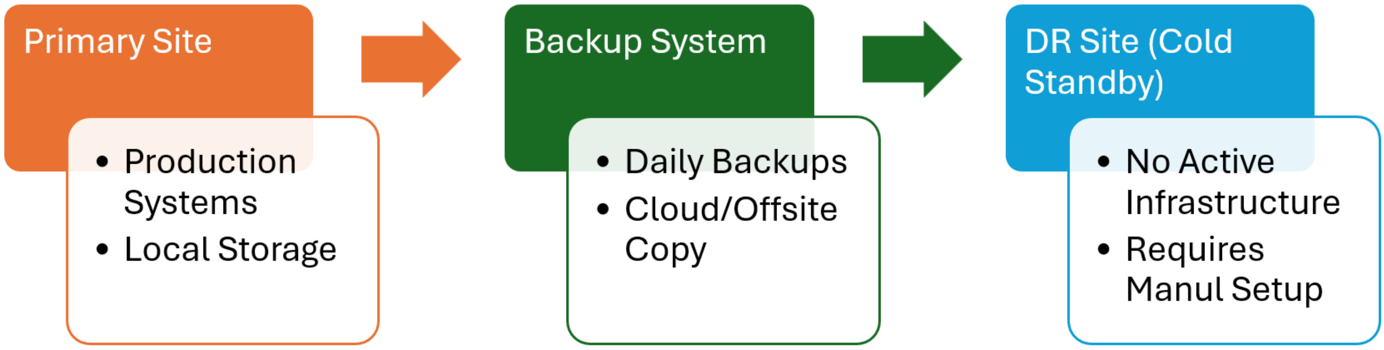
- Preconfigured Infrastructure
- Not Active but ready
- Auto Failover support

Scenario 2: RPO = 24 Hours; RTO = 72 Hours; High Availability Not Required

This DR strategy is suitable for non-critical or internal systems that can tolerate downtime for up to three days and up to 24 hours of data loss. It typically uses cold standby infrastructure with backup based recovery, favouring cost effectiveness over speed.

Typical Applications:

- Internal email systems
- HR platforms and time-logging tools
- Batch finance or payroll systems
- File shares and document management systems



Primary Site

- Production Systems
- Local Storage

Backup System

- Daily Backups
- Cloud/Offsite Copy

DR Site (Cold Standby)

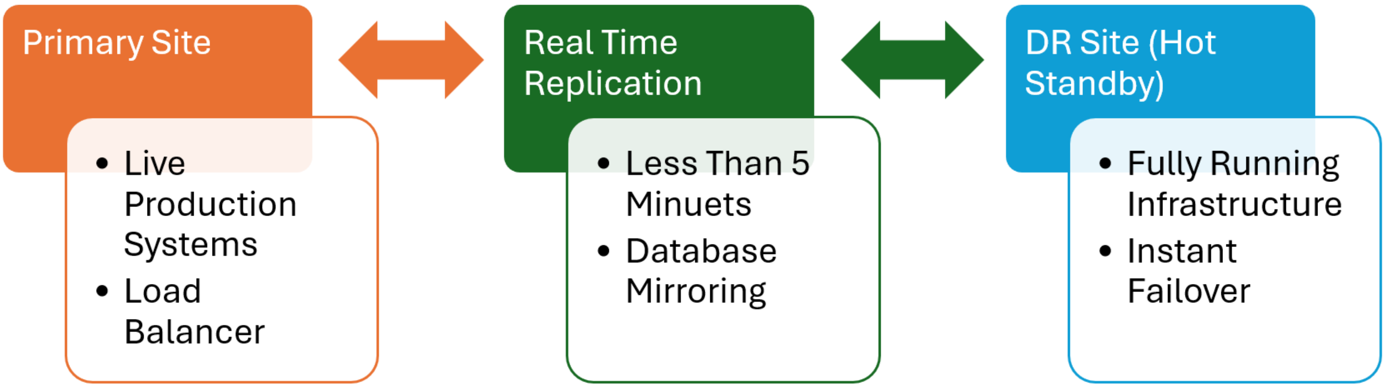
- No Active Infrastructure
- Requires Manul Setup

Scenario 3: RPO = 5 Minutes; RTO = 1 Hour; High Availability Required

This high-end scenario targets mission-critical, real-time systems where downtime or data loss must be virtually non-existent. It utilises a hot standby setup, with real-time replication.

Typical Applications:

- Online banking systems
- Payment gateways and checkout systems
- Live stock or trading platforms
- Real-time dashboards or telemetry services



References

Alcántara, A.V. (2020) *Design and implementation of a disaster recovery plan in a small company*. Available at: https://core.ac.uk/download/pdf/350765431.pdf (Accessed: 11 April 2025).

Cloudian (no date) *4 Disaster Recovery Plan Examples and 10 Essential Plan Items*. Available at: https://cloudian.com/guides/disaster-recovery/4-disaster-recovery-plan-examples-and-10-essential-plan-items/ (Accessed: 11 April 2025).

IBM (no date) *Example of a disaster recovery plan*. Available at: https://www.ibm.com/docs/en/i/7.6.0?topic=system-example-disaster-recovery-plan (Accessed: 11 April 2025).

Morrow, T., LaPiana, V., Faatz, D., Hueca, A. and Richmond, N. (2021) *Cloud Security Best Practices Derived from Mission Thread Analysis*. Available at: https://apps.dtic.mil/sti/pdfs/AD1139951.pdf (Accessed: 11 April 2025).