

DRC — Disaster Recovery Center

Ensuring Business Continuity in the Event of a Disaster

In today's digital world, data is every organization's most valuable asset. Earthquakes, fires, floods, and cyberattacks can destroy years of critical information in seconds. This is where the Disaster Recovery Center (DRC) plays a vital role — an essential component of modern IT governance that guarantees uninterrupted service delivery under any disaster scenario.



What Is a DRC?

A Disaster Recovery Center (DRC) is a secondary IT infrastructure that mirrors an organization's critical systems. When the primary data center becomes unavailable for any reason, the DRC — located in a geographically separate site — takes over operations and maintains business continuity.



Primary Data Center

Handles all daily operations and live workloads.



DRC — Disaster Recovery Center

Activates automatically when the primary site fails.

A notable Turkish example: Istanbul Metropolitan Municipality (IMM/İBB) established a DRC in Ankara in 2023 to protect city data against earthquakes and major disasters. Critical public services for Istanbul can continue uninterrupted even during a catastrophic event.

How a DRC Works

A DRC operates on three core pillars: data backup, replication, and automated failover.

1. Data Backup

Data is regularly copied to offsite locations and kept ready for activation.

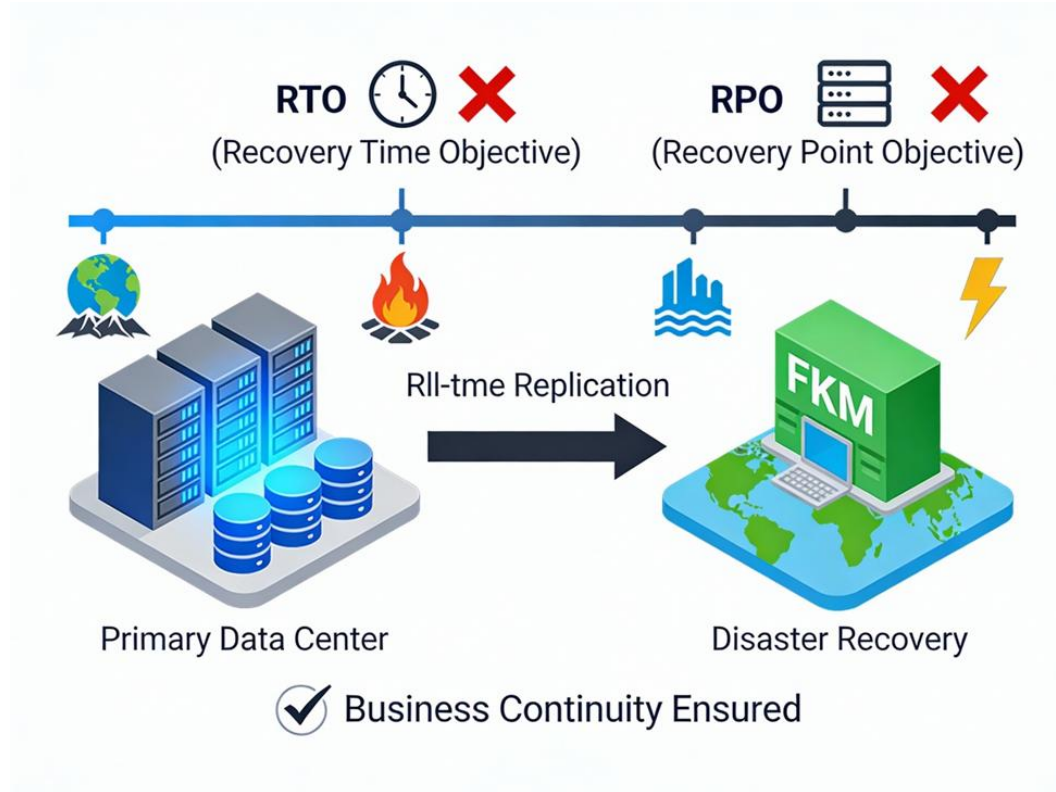
- Cloud-based: AWS, Azure, Google Cloud
- Physical: Secondary data centers in different cities

2. Data Replication

Maintains multiple synchronized copies of data at all times.

- Synchronous — Instant mirror write, near-zero data loss. Ideal for banks and critical infrastructure.
- Asynchronous — Batched interval sync. Faster throughput with a small acceptable data-loss window.

RTO & RPO: The Critical DRC Metrics



RTO — Recovery Time Objective

How quickly systems must be restored after a disaster.

- ▶ Critical systems: 15 minutes
- ▶ Important systems: 1–4 hours
- ▶ Standard systems: 8–24 hours

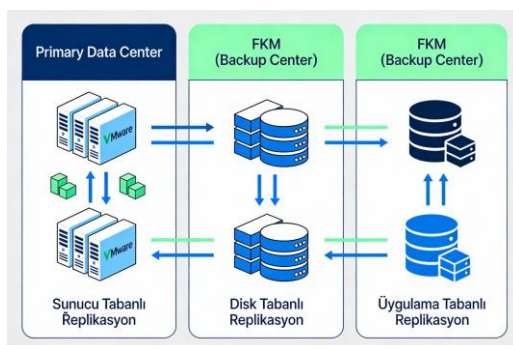
RPO — Recovery Point Objective

Maximum acceptable data loss measured in time.

- ▶ Financial transactions: 0–15 min (near real-time)
- ▶ Customer database: 30–60 min
- ▶ Archival data: 24 hours

💡 The shorter the RTO, the more investment is required in hot-standby systems — which directly raises infrastructure costs. Setting realistic RTO/RPO values based on actual business requirements is essential for cost-effective DRC design.

Replication Technologies Used in DRC



Server-Based Replication

Entire virtual machines are replicated to the DRC using tools such as VMware SRM (Site Recovery Manager). Enables automated failover from primary to backup site. Easy to implement and widely adopted.

Storage-Based Replication

All or selected storage volumes are replicated to the DRC. Primary and backup sites must use compatible storage hardware from the same vendor. Common solutions: EMC

RecoveryPoint, Veeam Backup & Replication.

Application-Based Replication

Databases and software applications natively push data to the DRC. Lower upfront cost, but software licensing and support requirements may offset the expected savings.

Key Advantages of a DRC

 Business Continuity Services stay online even during major disasters.	 Customer Trust Continuous availability preserves client confidence and SLAs.	 Regulatory Compliance Banks and financial institutions are legally required to maintain a DRC.
 Financial Protection Minimizes losses caused by data loss or downtime.	 Competitive Edge Crisis-resilient organizations protect and grow market share.	 Cyber Resilience Clean recovery point following ransomware or cyberattacks.

TR DRC Case Studies in Turkey

Istanbul Metropolitan Municipality (IMM) ▶ DRC established in Ankara in 2023 ▶ All critical IMM data backed up regularly ▶ Activated in case of earthquake, flood, or fire ▶ Ensures uninterrupted public services for Istanbul	Government Agencies & Universities ▶ AFAD operates AYDES — nationwide disaster management platform ▶ Coordinates emergency response across all provinces ▶ Dumlupınar University and others run their own DRC systems ▶ Growing DRC adoption trend across the public sector
--	--

DRC Planning: Eight Essential Steps

1 Risk Analysis Identify disaster scenarios your organization may face.	2 Critical Systems Inventory Determine which data and systems require priority protection.
3 Define RTO & RPO Set recovery parameters aligned with actual business	4 Technology Selection Choose server-based, storage-based, or application-

requirements.

5 Infrastructure Setup

Deploy physical servers, storage arrays, and network devices at the DRC site.

7 Staff Training

Train IT personnel on DRC activation, failover, and management procedures.

based replication.

6 Disaster Drills

Simulate failure scenarios and verify recovery procedures end-to-end.

8 Ongoing Maintenance

Schedule regular updates, audits, and tests of all DRC components.

LANDE T.R.O.Y.A Solution for DRC Infrastructure

Modern DRC environments require IT equipment to be housed securely, organized efficiently, and accessible rapidly. The T.R.O.Y.A (Next Generation Datacenter Cabinet) system developed by LANDE is a purpose-built solution for exactly these demands.

T.R.O.Y.A acts as the backbone of any DRC infrastructure — keeping data center equipment secure, organized, and always accessible.

-  Seismic Resistance — Special seismic platform protects equipment during earthquakes
-  High Density — Maximizes rack unit utilization within limited floor space
-  Smart Airflow — Optimizes cooling efficiency with managed airflow design
-  Physical Security — Electronic locks and access control for all critical equipment



Conclusion

A Disaster Recovery Center is a mission-critical system for safeguarding an organization's digital assets. With correctly defined RTO/RPO parameters, the right technology stack, and regular testing, organizations can maintain business continuity under any disaster scenario.

Given Turkey's seismic risk, DRC investments are no longer optional — they are a mandatory operational necessity. Following the example of Istanbul Metropolitan Municipality, both public institutions and private-sector organizations should develop and implement their own DRC strategy.

"Every second of downtime costs money, trust, and reputation. A DRC does not just protect data — it protects the business itself."