04 · PROTECT · BACKUP & DISASTER RECOVERY

We measure in advance how many minutes it will take you to recover from a disaster.

From an organisation-specific backup policy to a Data Guard-based disaster recovery architecture, from regular restore tests to a step-by-step DR runbook, we safeguard your business continuity.

THE PROBLEM WE SOLVE

Backups are taken, but nobody knows when a restore was last tested.

It is unclear what happens if ransomware encrypts the backups too.

RTO and RPO targets are written down but have never been measured.

SCOPE OF SERVICES

Backup policy
Design of an organisation-specific backup policy and retention planning.

Immutable backup architectures
Copies protected against ransomware with RMAN, snapshots and immutable backups.

Restore tests
Verifying through regular restore tests that backups really work.

Backup integration
Integration with NetWorker, ZFS and cloud storage infrastructures.

DR architecture
Disaster recovery with Data Guard and platform-independent replication, including Exadata-to-Exadata.

RTO / RPO design
Designing recovery time and data loss tolerance according to business continuity objectives.

TECHNOLOGIES

Oracle Database · Exadata / ExaCC · Microsoft SQL Server · PostgreSQL / EDB · OLVM / KVM · RMAN · Data Guard · NetWorker · ZFS

QUICK START

Package	Duration	Deliverables
DR Drill	1 week	Measured RTO/RPO and an up-to-date runbook

Free discovery call

We spend 45 minutes understanding your environment and priorities. Free of charge.

CONTACT

info@turncloudon.com

0850 346 30 49

www.turncloudon.com.tr/en/uzmanlik/yedekleme-fkm

Istanbul · Ankara · Konya · Prague

METHOD

01
Policy and Inventory
Mapping critical systems and the current backup setup.

02
Architecture
Designing the backup and DR architecture according to RTO/RPO targets.

03
Implementation
Deploying the backup, replication and monitoring infrastructure.

04
Drills
Planned switchover and failover drills, with timings measured.

05
Runbooks and Training
Step-by-step DR runbook documentation and team training.

THREE TIERS BUILT ON RPO AND RTO

Package	RPO	RTO	Backup schedule	Suitable workloads
Standard	24 hours	8 hours	Daily incremental, weekly full; 30-day retention, monthly archive for 12 months	File servers, secondary applications, test environments
Advanced	4 hours	4 hours	Daily full + intraday incremental, log backups for databases; 90-day retention	Business applications, medium-criticality databases
Critical	15 minutes	1 hour	Continuous log/WAL archiving, point-in-time recovery, copy to a second site	Production databases, business-critical applications

Values are finalised by workload class in the annex to the service agreement.

THE 3-2-1-1-0 RULE

- Three copies, two different media, one off-site, one immutable, zero verification errors
- Undeletable copy with object lock or WORM
- The backup system is authorised independently of the production identity infrastructure
- Encryption in transit and at rest; key management is kept separate
- Integrity check of every backup and regular restore testing
- Scenario-based disaster recovery plan and at least two drills per year

MEASURABLE COMMITMENT

We do not consider a backup successful until it has passed a restore test. The monthly report includes the number of backups tested, the measured restore time and how it compares with the committed RTO.

SOLUTION DETAILS

High Availability and Replication	An uninterrupted data layer with Data Guard, Always On, Patroni and InnoDB Cluster; heterogeneous replication with GoldenGate.