Oracle Data Guard on Exadata (On-Prem) – Pre-Implementation Guide

This document provides a checklist of questions to answer before implementing Oracle Data Guard on an on-premises Exadata system. It also includes possible decisions and next steps depending on your requirements, both in English and German. A decision flowchart is provided at the end for quick guidance.

# 1. Data Guard Pre-Implementation Checklist (English)

## What is the Recovery Time Objective (RTO) and Recovery Point Objective (RPO)?

Low RTO/RPO (near zero) → Maximum Availability/Protection, Far Sync.  
Higher RPO acceptable → Maximum Performance.

## What is the main purpose of the standby database?

Disaster Recovery → Physical Standby.  
Reporting → Active Data Guard license required.  
Testing → Snapshot Standby.  
Heterogeneous platform → Logical Standby.

## How many standby databases are required?

One standby → Standard configuration.  
Multiple → Cascading standby or Far Sync.

## Will Fast-Start Failover (FSFO) be required?

Yes → Needs Data Guard Broker + Observer.  
No → Manual switchover/failover.

## Where will the standby reside?

Same datacenter → Protects against server/rack failures.  
Remote site → Requires dedicated bandwidth, encryption/compression.

## What is the available network bandwidth/latency?

High bandwidth, low latency → Synchronous redo transport.  
Low bandwidth, high latency → Asynchronous with compression.

## What Exadata shapes/versions are used?

Same generation/version → Compatible.  
Different → Ensure same Oracle DB version/patch.

## Is the database CDB/PDB (Multitenant)?

Yes → Protect all PDBs or PDB-level DG (12.2+).  
No → Classic single DB.

## What is the redo generation rate?

High → Sufficient SRLs, compression, network sizing.  
Low/Medium → Standard SRLs.

## How will backups be handled?

Primary only → Simpler, but production load.  
Standby offload (Active DG) → Needs license.

## Will Active Data Guard be licensed?

Yes → Reporting, backups, corruption detection.  
No → Mount-only standby.

## What is the switchover/failover procedure?

Manual DBA-driven.  
Automated → FSFO + DG Broker.

## How will monitoring be done?

OEM/Cloud Control.  
Custom scripts.  
DG Broker.

## How will patching be managed?

Rolling patching (apply to standby first).  
Non-rolling → Downtime.

## Is redo transport encryption required?

Yes → Native encryption/TLS.  
No → Only if secure network.

## Are compliance/read-only reporting needs important?

Yes → Active Data Guard.  
No → DR standby only.

# 2. Data Guard Vorbereitungs-Checkliste (Deutsch)

## Was sind die Wiederanlaufzeit (RTO) und der Datenverlust (RPO)?

Sehr niedrig (nahe null) → Maximum Availability/Protection, Far Sync.  
Höher akzeptabel → Maximum Performance.

## Welcher Zweck hat die Standby-Datenbank?

Disaster Recovery → Physisches Standby.  
Reporting → Active Data Guard Lizenz.  
Test/QA → Snapshot Standby.  
Heterogenes System → Logisches Standby.

## Wie viele Standby-Datenbanken werden benötigt?

Eine → Standard.  
Mehrere → Kaskadierend oder Far Sync.

## Wird Fast-Start Failover (FSFO) benötigt?

Ja → Data Guard Broker + Observer.  
Nein → Manuelles Umschalten.

## Wo steht das Standby-System?

Gleiches Rechenzentrum.  
Anderer Standort → Bandbreite, Verschlüsselung, Komprimierung.

## Welche Netzwerkbandbreite/Latenz steht zur Verfügung?

Hoch/niedrig → Synchron möglich.  
Niedrig/hoch → Asynchron mit Komprimierung.

## Welche Exadata-Versionen sind im Einsatz?

Gleich → Kompatibel.  
Unterschiedlich → Gleiche DB Version/Patchlevel.

## Ist die DB CDB/PDB (Multitenant)?

Ja → Alle PDBs oder PDB-Level DG.  
Nein → Klassisch.

## Wie hoch ist die Redo-Generierung?

Hoch → SRLs, Komprimierung, Netz.  
Niedrig/Mittel → Standard-SRLs.

## Wie werden Backups durchgeführt?

Nur Primär → Einfach.  
Auf Standby (Active DG) → Lizenz nötig.

## Wird Active Data Guard lizenziert?

Ja → Reporting, Backups, Block-Prüfung.  
Nein → Mount-Only.

## Wie läuft das Umschalten/Failover ab?

Manuell oder Automatisiert (FSFO).

## Wie wird überwacht?

OEM/Cloud Control, Skripte, DG Broker.

## Wie erfolgt das Patching?

Rolling (Standby zuerst).  
Nicht-Rolling → Downtime.

## Muss Redo verschlüsselt sein?

Ja → Netzwerkverschlüsselung/TLS.  
Nein → Nur sicheres Netz.

## Ist Compliance/Reporting wichtig?

Ja → Active DG.  
Nein → Nur DR.

# 3. Decision Flowchart

The following decision flowchart guides you in selecting the right Data Guard setup:  
  
1. Define RTO/RPO → If near zero, use Maximum Availability/Protection; otherwise Maximum Performance.  
2. Purpose of standby → DR = Physical Standby, Reporting = Active DG, Testing = Snapshot Standby.  
3. Number of standbys → If >1, consider Cascading Standby or Far Sync.  
4. Bandwidth/Latency → High = Synchronous, Low = Asynchronous with compression.  
5. Automation → If FSFO needed, enable DG Broker.  
6. Backup/Reporting needs → If yes, license Active DG.  
7. Compliance/Encryption → Enable redo transport encryption if required.