AnovaCloud

FREE PRACTITIONER PACK

SQL Server → PostgreSQL Migration Pack

Eighteen checks. Nothing proceeds until every box is honestly ticked.

Pack	SQL Server → PostgreSQL Migration Pack
Document	Security assessment (18 checks)
Date	2026-09

HOW TO USE

How to use

Assign an owner per check. A check is done when there is evidence — a script, a diagram, a rehearsal log — not when someone says it is.

ASSESSMENT CHECKS

Assessment checks

- [ ] **Login inventory**
  Every server login cataloged: type (Windows/SQL), purpose, owner, last used.
- [ ] **Windows/AD auth path**
  Target auth decided: LDAP, Kerberos, or IdP-backed; no silent fallback to shared SQL logins.
- [ ] **Orphaned users identified**
  Users without matching logins found per database; SID remap plan written.
- [ ] **Server roles reviewed**
  sysadmin membership minimized; each privileged login has a named owner and justification.
- [ ] **Database roles & grants**
  Role membership and object grants scripted; least-privilege re-applied on PostgreSQL (no blanket db_owner).
- [ ] **Contained databases noted**
  Contained users converted to PostgreSQL roles with explicit passwords or cert auth.
- [ ] **Row-level security**
  SQL Server RLS policies re-implemented as PostgreSQL RLS policies and tested per role.
- [ ] **Data masking**
  Dynamic data masking replaced (application-layer or anonymizer extension); masked columns listed.
- [ ] **Always Encrypted**
  Columns using Always Encrypted have a target design: pgcrypto, application encryption, or HSM.
- [ ] **TDE**
  Transparent Data Encryption replaced with filesystem/volume encryption or pgcrypto; key custody defined.
- [ ] **Certificates & keys**
  All certificates, asymmetric/symmetric keys inventoried with rotation plan on the target.
- [ ] **Auditing**
  SQL Server Audit specs mapped to pgaudit or platform logging; audit retention meets compliance.
- [ ] **Service accounts**
  SQL Server and Agent service accounts replaced with least-privilege PostgreSQL/OS accounts.
- [ ] **Password policy**
  Password complexity, expiry, and lockout enforced on PostgreSQL roles (check extension support).
- [ ] **Network & firewall**
  Target firewall rules, private endpoints, and TLS enforcement defined before first data moves.

- [ ] **Secrets management**
  All credentials in the vault; no connection strings with passwords in code or configs.
- [ ] **Vulnerability baseline**
  Source hardened baseline documented; target scanned before cutover.
- [ ] **Compliance sign-off**
  Data residency, encryption, and audit requirements signed off for the PostgreSQL topology.