# Flowchart

**Permission Request** → **Solution Owner Approval** → **Workflow: Database Schema Access Request** → **Are groups present in AD?**

- **YES** → **Group Membership Edits performed by IT Systems / Cyber *NO DBA ACTION REQUIRED*** → **Are groups mapped in SQL?**
  - **YES** → **Customer Verification**
  - **NO** → **Workflow: DBMS Access Request**
- **NO** → **Workflow: AD / Entra Account / Group Creation Request** → (back to Workflow: Database Schema Access Request)

**Workflow: DBMS Access Request** →

**Add Login (Group)** → **List of Server Roles** → **Apply Permissions (*as necessary*)** → **Workflow: Database Access Request** → **Add User (Group)** → **List of DB Permissions*** → **Apply Schema Permissions** → (Customer Verification)

- *Default membership to public (connect) server instance role* (under Add Login (Group))
- *Default membership to public (connect) DB role* (under Add User (Group))

**\*Please note** that Role Based Access Controls (RBAC) at the database schema level are not natively available within SQL Server. Permissions are explicitly granted to each group as necessary.

---

**"DEFAULT" GROUPS PER SCHEMA:**

**LEGEND:**
P-SQL-<SOLUTIONABBREV>-<SDLCSCOPE>-<SCHEMANAME>_<PERMISSIONDESC>

**EXAMPLES:**
P-SQL-EDW-PRD-ecrm-reader – ("*read only to ecrm schema in EDW*")
P-SQL-EDW-PRD-ecrm-unmaskedreader – ("*can unmask and read sensitive attributes within ecrm schema in EDW*")
P-SQL-EDW-PRD-ecrm-writer – ("*write access to ecrm schema in EDW*")
P-SQL-EDW-PRD-ecrm-owner – ("*can do 'everything' within ecrm schema in EDW*")
P-SQL-EDW-PRD-ecrm-executor – ("*can execute stored procedures within ecrm schema in EDW*")

---

**DECISION FLOW 1**

BEGIN

1. Access is required to the database schema layer of a solution
2. The solution owner (or a delegate) approves or denies
3. Begin workflow
4. Do the 5 ActiveDirectory / Entra security groups that provide access to the database schema exist?
5. If YES, with written approval from schema creator / owner attached, Cyber adds AD / Entra user account to AD / Entra security groups that correspond with the level of access required to database schemas.
6. Cyber forwards request to DBA group to verify mapping of AD / Entra security group to database schema.
7. Verify access granted.

END

**DECISION FLOW 2**

BEGIN

1. Access is required to the database schema layer of a solution
2. The solution owner (or a delegate) approves or denies
3. Begin workflow
4. Do the 5 ActiveDirectory / Entra security groups that provide access to the database schema exist?
5. If NO, revert to **AD / Entra Account / Group Creation Request** workflow
6. Upon creation of the 5 AD / Entra groups:
7. Revert to **DBMS Access Request**
8. Link to **Database Access Request**
9. DBA maps explicit schema level permissions to AD / Entra security groups.
10. Verify access granted

END