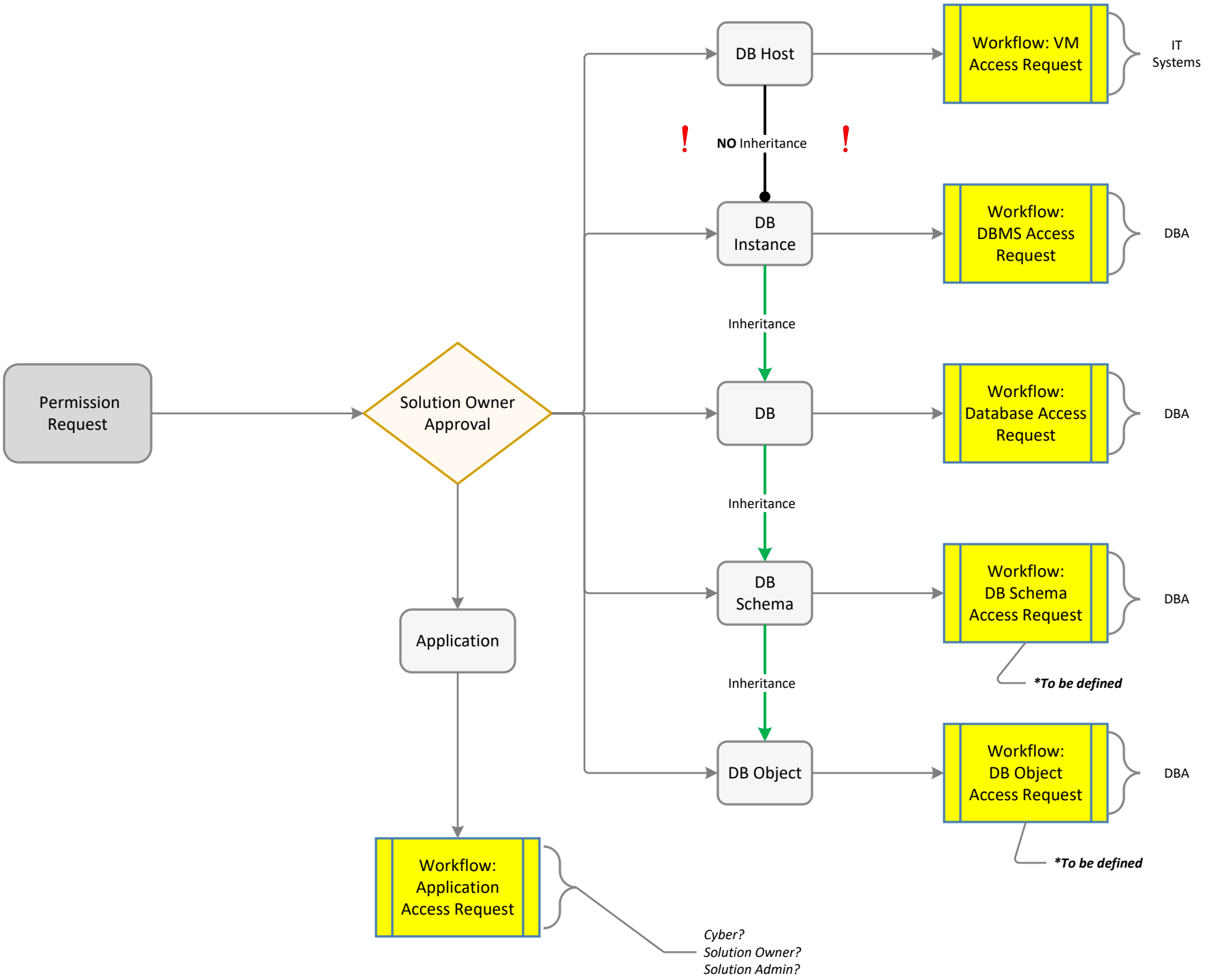
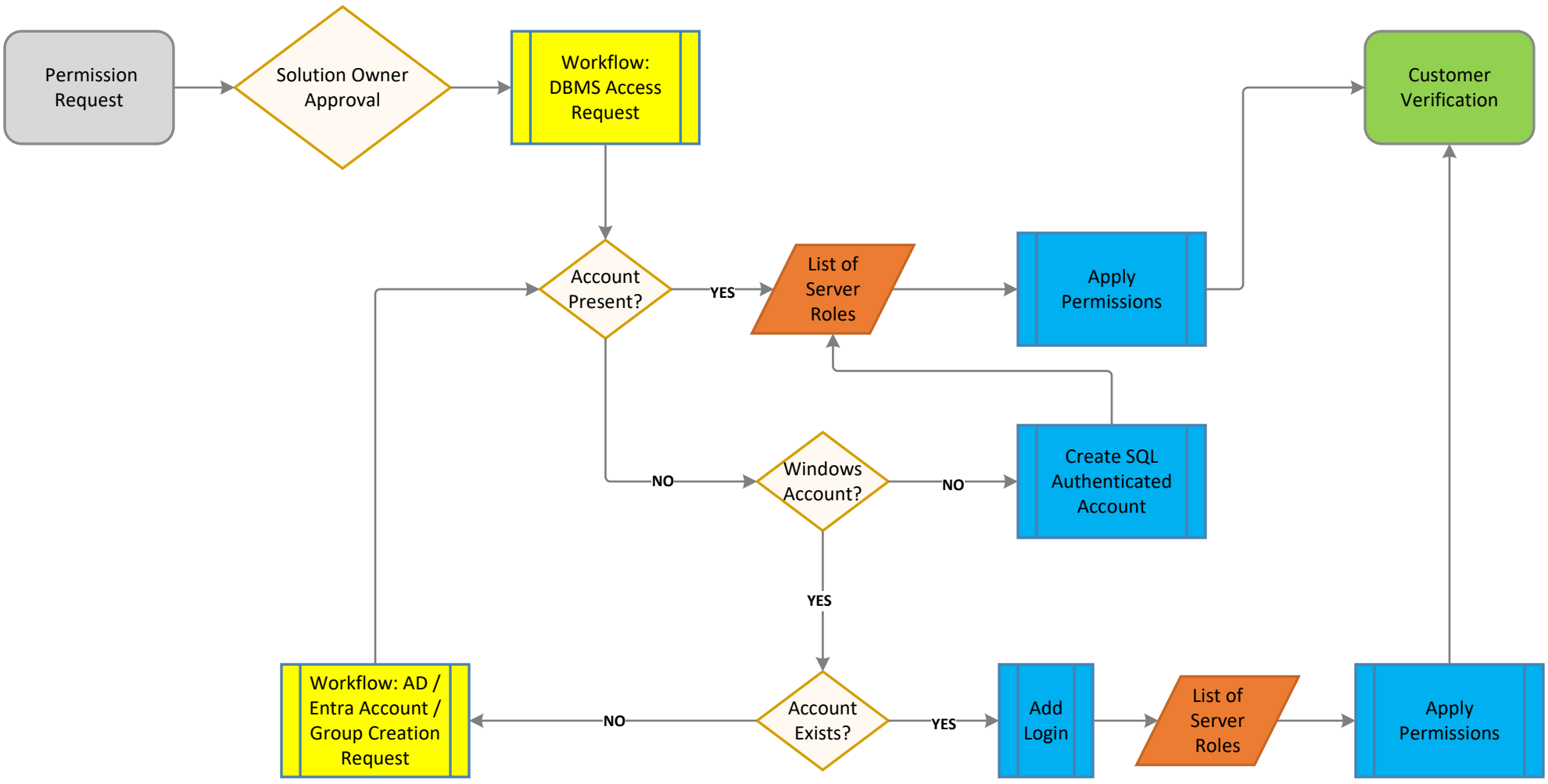

Permission Request
Solution Owner Approval
Application
Workflow: Application Access Request
Cyber?
Solution Owner?
Solution Admin?
DB Host
NO Inheritance
DB Instance
Inheritance
DB
Inheritance
DB Schema
Inheritance
DB Object
Workflow: VM Access Request
IT Systems
Workflow: DBMS Access Request
DBA
Workflow: Database Access Request
DBA
Workflow: DB Schema Access Request
DBA
*To be defined
Workflow: DB Object Access Request
DBA
*To be defined



DECISION FLOW 1

BEGIN

1. A user requires “access” to the database layer of a solution
2. The solution owner (or a delegate) approves or denies
3. Begin workflow
4. Is the account (tech: “the login”) present on the DBMS instance?
5. If **YES**, display list of available server roles to be applied.
6. Select role(s).
7. Apply Permissions.
8.Verify access granted.

END

DECISION FLOW 2

BEGIN

1. A user requires “access” to the database layer of a solution
2. The solution owner (or a delegate) approves or denies
3. Begin workflow
4. Is the account (tech: “the login”) present on the DBMS instance?
5. If **NO**, is account type a Windows (aka *“Domain”, “Active Directory”*) Account?
6. If **NO**, create SQL Server Authenticated Account.
7. Display list of available server roles to be applied.
8. Select role(s).
9. Apply Permissions.
10.Verify access granted.

END

DECISION FLOW 3

BEGIN

1. A user requires “access” to the database layer of a solution
2. The solution owner (or a delegate) approves or denies
3. Begin workflow
4. Is the account (tech: “the login”) present on the DBMS instance?
5. If **YES**, is account type a Windows (aka *“Domain”, “Active Directory”*) Account?
6. If **YES**, is account present within Active Directory / Entra?
7. If **YES**, add account (tech: “the login”) to SQL Server
8. display list of available server roles to be applied.
9. Select role(s).
10. Apply Permissions.
11.Verify access granted.

END

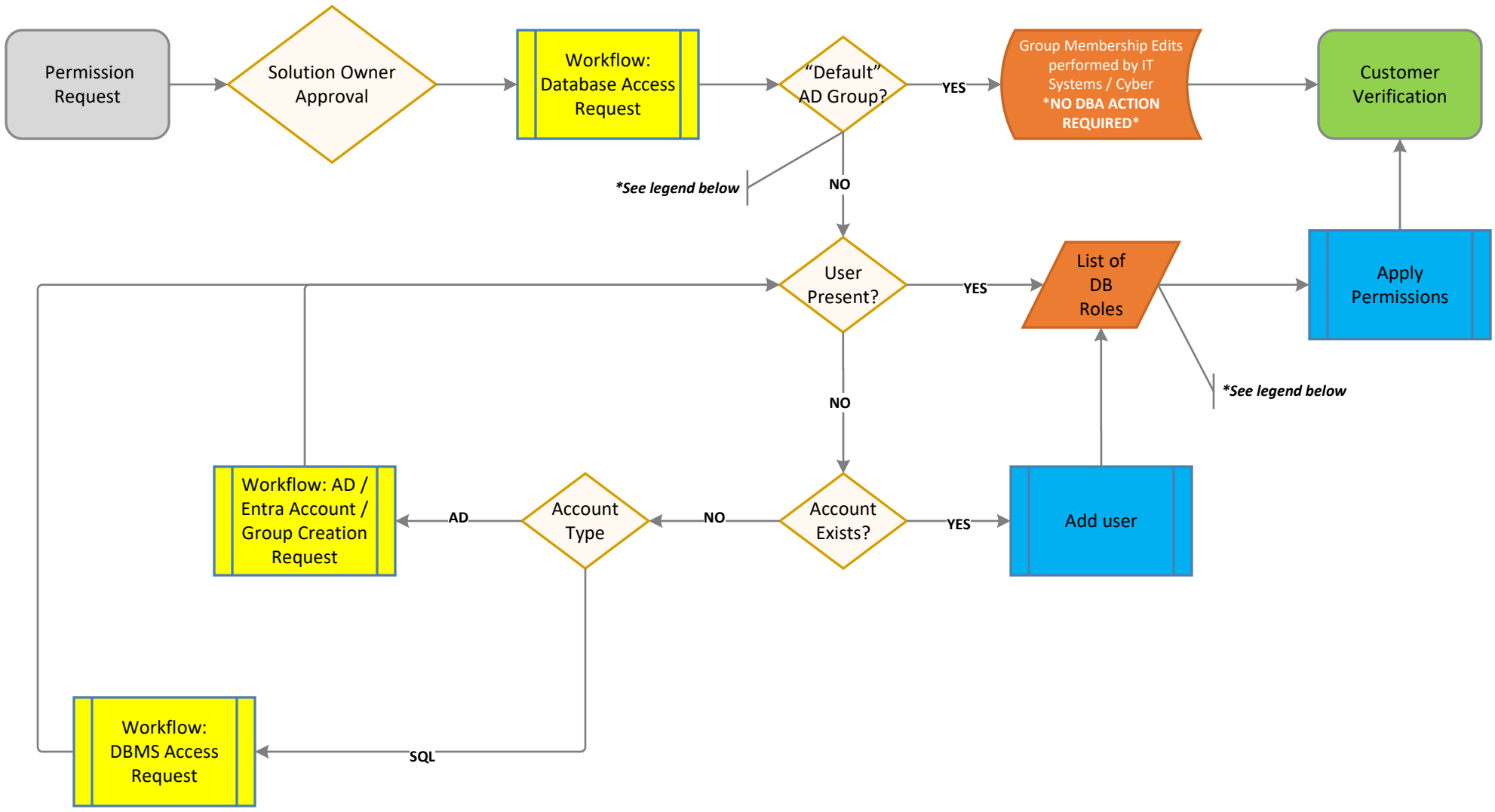
DECISION FLOW 4

BEGIN

1. A user requires “access” to the database layer of a solution
2. The solution owner (or a delegate) approves or denies
3. Begin workflow
4. Is the account (tech: “the login”) present on the DBMS instance?
5. If **NO**, is account type a Windows (aka *“Domain”, “Active Directory”*) Account?
6. If **YES**, is account present within Active Directory / Entra?
7. If **NO**, begin workflow to create account within Active Directory / Entra.
8. Revert to **DECISION FLOW 3, Step 6.**
9. Continue to verification

END

END



"DEFAULT" GROUPS PER SOLUTION:

LEGEND:
P-SQL-<SDLCSCOPE>-<SOLUTIONSCOPE>-<DEFAULTORCUSTOM>_<DBROLEDESC>

EXAMPLES:
P-SQL-PRD-RogueOne-default_datareader – ("*read only*")
P-SQL-PRD-RogueOne-default_datawriter – ("*write access*")
P-SQL-PRD-RogueOne-default-dbowner – ("*dbo*")
P-SQL-PRD-RogueOne-custom_executor – ("*can execute stored procedures*")

Default Database Roles Available *(per database)*:

db_datareader – (*grants read access*)
db_datawriter – (*grants write access*)
db_ddladmin – (*grants object modification ability*)
db_owner – (*grants *all* writes within database*)
***db_sp_executor** – (*grants ability to execute stored procedures (*custom role)*)

DECISION FLOW 1

BEGIN

1. Access is required to the database layer of a solution
2. The solution owner (or a delegate) approves or denies
3. Begin workflow
4. Is the level of access being requested for a user to have "read", "write", "execute stored procedures against", or "full control" to all of the databases that support this solution?
5. If YES, forward request to Cyber to add the user account to the corresponding Active Directory / Entra security group.
6.Verify access granted.

END

DECISION FLOW 2

BEGIN

1. Access is required to the database layer of a solution
2. The solution owner (or a delegate) approves or denies
3. Begin workflow
4. Is the level of access being requested for a user to have "read", "write", "execute stored procedures against", or "full control" to all of the databases that support this solution?
5. If NO, is the user already mapped to the database(s) supporting the solution in question?
6. If YES, display list of available database roles to be applied.
7. Select role(s).
8. Apply Permissions.
9 .Verify access granted.

END

DECISION FLOW 3

BEGIN

1. Access is required to the database layer of a solution
2. The solution owner (or a delegate) approves or denies
3. Begin workflow
4. Is the level of access being requested for a user to have "read", "write", "execute stored procedures against", or "full control" to all of the databases that support this solution?
5. If NO, is the user already mapped to the database(s) supporting the solution in question?
6. If NO, is the account (tech: "the login") already present on the SQL Server instance?
7. If YES, map the user to the database(s) supporting the solution.
8. Display list of available database roles to be applied.
9. Select role(s).
10. Apply Permissions.
11 .Verify access granted.

END

DECISION FLOW 4

BEGIN

1. Access is required to the database layer of a solution
2. The solution owner (or a delegate) approves or denies
3. Begin workflow
4. Is the level of access being requested for a user to have "read", "write", "execute stored procedures against", or "full control" to all of the databases that support this solution?
5. If NO, is the user already mapped to the database(s) supporting the solution in question?
6. If NO, is the account (tech: "the login") already present on the SQL Server instance?
7. If NO, should the account use Windows credentials to authenticate to the Database(s) that support(s) the solution?
8. If YES, does the account already exist within Windows (aka "the Domain", "Active Directory")?
9. If YES, add account (tech: "the login") to SQL Server
10. Map the user to the database(s) supporting the solution.
11. Display list of available database roles to be applied.
12. Select role(s).
13. Apply Permissions.
14 .Verify access granted.

END

DECISION FLOW 5

BEGIN

1. Access is required to the database layer of a solution
2. The solution owner (or a delegate) approves or denies
3. Begin workflow
4. Is the level of access being requested for a user to have "read", "write", "execute stored procedures against", or "full control" to all of the databases that support this solution?
5. If NO, is the user already mapped to the database(s) supporting the solution in question?
6. If NO, is the account (tech: "the login") already present on the SQL Server instance?
7. If NO, should the account use Windows credentials to authenticate to the Database(s) that support(s) the solution?
8. If YES, does the account already exist within Windows (aka "the Domain", "Active Directory")?
9. If NO, begin workflow to create account within Active Directory / Entra.
10. Revert to DECISION FLOW 4, Step 8.
11. Continue to verify access granted.

END

DECISION FLOW 6

BEGIN

1. Access is required to the database layer of a solution
2. The solution owner (or a delegate) approves or denies
3. Begin workflow
4. Is the level of access being requested for a user to have "read", "write", "execute stored procedures against", or "full control" to all of the databases that support this solution?
5. If NO, is the user already mapped to the database(s) supporting the solution in question?
6. If NO, is the account (tech: "the login") already present on the SQL Server instance?
7. If NO, should the account use Windows credentials to authenticate to the Database(s) that support(s) the solution?
8. If NO, revert to DBMS Access Request (D2S6).
9. THEN revert to Database Access Request (D3S6)
10. Continue to verify access granted.

END