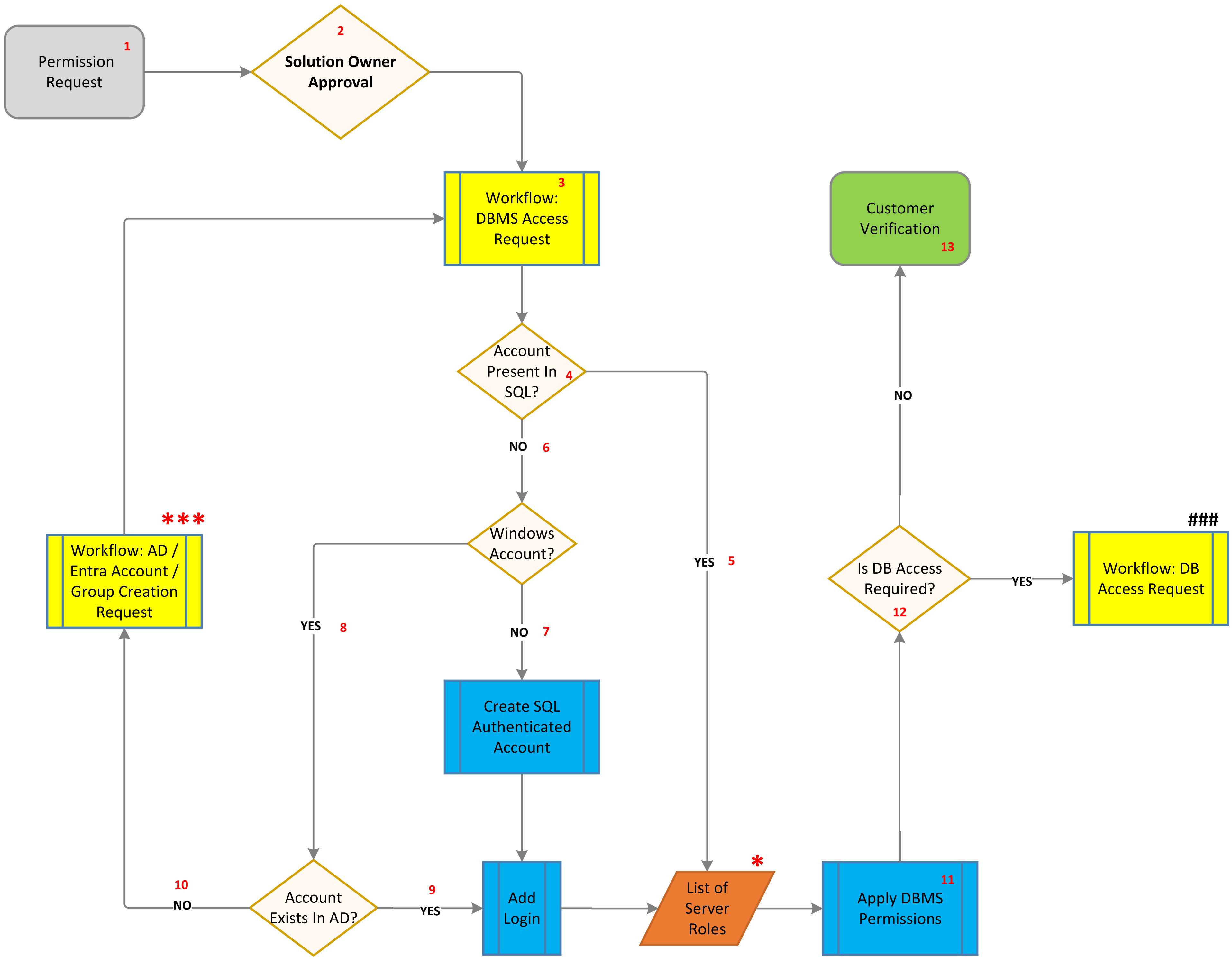
Permission Request 1
2 Solution Owner Approval
3 Workflow: DBMS Access Request
Customer Verification 13
Account Present In SQL? 4
NO 6
YES 5
Windows Account?
YES 8
NO 7
Create SQL Authenticated Account
***
Workflow: AD / Entra Account / Group Creation Request
10 NO
Account Exists In AD?
9 YES
Add Login
*
List of Server Roles
11 Apply DBMS Permissions
NO
Is DB Access Required? 12
YES
###
Workflow: DB Access Request

1. A user requires access to the Database Management System (DBMS) layer of a solution

2. The owner of a solution being hosted by the SQL Server Platform (*or a delegate*) approves or denies the access request
   a. **NOTE**: The requestor's manager is **NOT** an appropriate / sufficient approver for this request.
   b. If the solution owner is unknown, there should be an informal effort to determine who owns the data that is supported by a database that the user is requesting access to.
   c. Once solution ownership is definitively determined, it should be recorded (*the "MAL" or a Solutions / Services ownership list?*).

3. Upon Solution Owner Approval, begin this workflow

4. "***Account Present In SQL?***": Is the account (*technically - "the login"*) already present on the DBMS instance?

5. If **YES**, the type of account is already known, and this attribute does not require specification by the requestor.

   *Display the list of DBMS ("Server") roles that can be granted to the account, which should be specified (or described) by the requestor.

6. If **NO**, the type of account to be added should be specified. Authentication / Connecting to SQL Server is possible through 2 methods; Windows AD / Microsoft Entra Authentication, or SQL Server Authentication. The requestor should specify the type required per their specific needs.

7. If the type specified is a SQL Server Authenticated Account, it is the responsibility of the DBA / DB Solutions group to **create** the account within SQL Server.

8. If the type specified is an AD / Entra Object, it is the responsibility of the DBA / DB Solutions group to **add** that object to SQL Server.

9. If the object is already present within AD / Entra, the object is added as a Login to SQL Server.

10. If the object does not yet exist within AD / Entra, it is the responsibility of the DBA / DB Solutions group to **create** that object within AD / Entra per the standards of the CyberSecurity Operations group, and the workflow they define to manage access to the AD / Entra subject area, **then** add that object to SQL Server.

    *****Due to this precedence constraint, diverting from the present workflow to that workflow should be a **required** action.

11. Upon creation of the object in AD / Entra, display the list of DBMS ("Server") roles that can be granted to the account, which should be specified (or described) by the requestor. The specified permissions to the DBMS layer of the solution are then applied.
    a. *I am comfortable deferring this attribute to be a general description, rather than selection from a list of native roles, due to the fact that the native roles are relatively obscure to most requestors.*

12. "***Is DB Access Required?***": Granting access to the DBMS layer of a solution does not automatically grant access to the databases that are hosted by the DBMS instance.

    ###If database access is required, it should be specified, and the user should be directed to the DB Access Request workflow as an **informational** attribute of the DBMS Access Request workflow. The present workflow should complete regardless.

13. Verify access granted. Workflow is complete. Ticket is closed.