

Project Design Phase-II

Data Flow Diagram & User Stories

DATE	27 OCT 2025
TEAM ID	NM2025TMID08298
PROJECT NAME	Optimizing User, Group, and Role Management with Access Control and Workflows
MAXIMUM MARK	4 Marks

Data Flow Diagrams:

Data Flow Diagram (DFD) Level 1 for the process of Optimizing User, Group, and Role Management (UGRM) with Access Control and Workflows. This visualization focuses on the key data transformations and interactions within a modern Identity Governance and Administration (IGA) system, often centered on a platform like ServiceNow.

Identity Creation (Top-Left Flow):

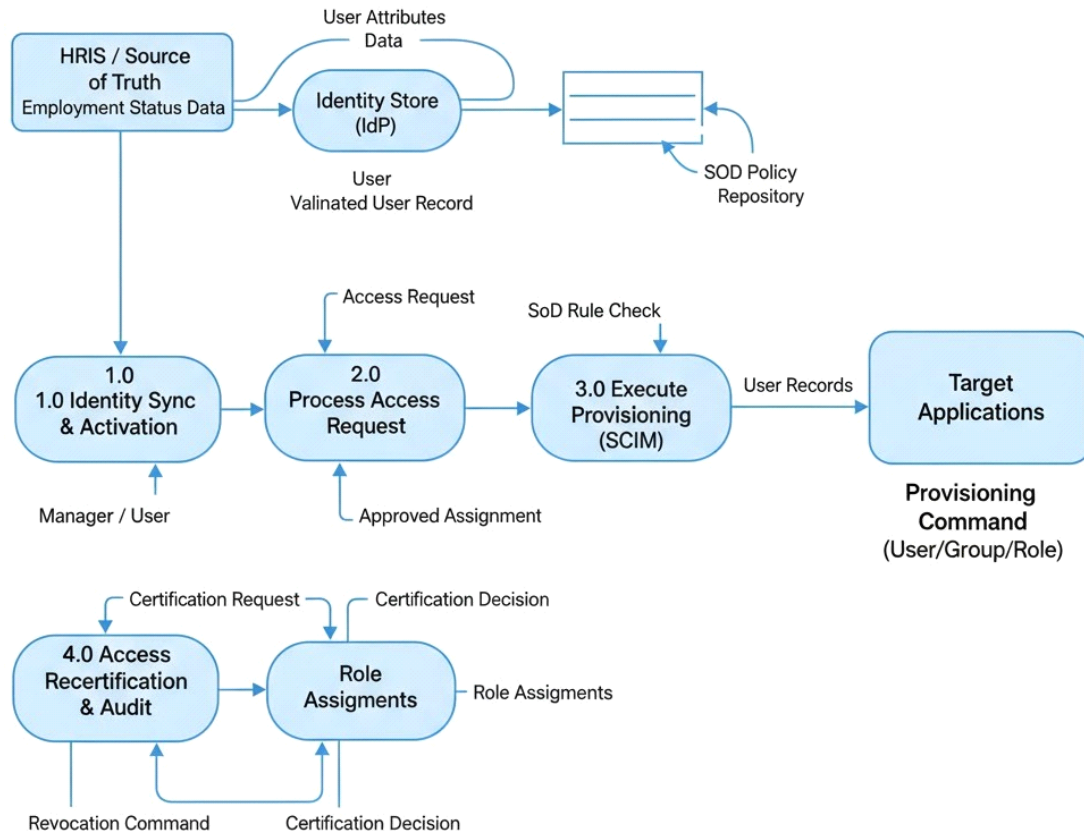
- An arrow labeled "**User Attributes**" flows from **HRIS / Source of Truth** (External Entity) into **Process 1.0 (Identity Sync & Activation)**.
- Process 1.0 pulls from the **Identity Store (IdP)** and writes a "**Validated User Record**" back into the store.

Access Request Flow (Central Path):

- An arrow labeled "**Access Request**" flows from **Manager / User** (External Entity) into **Process 2.0 (Process Access Request)**.
- Process 2.0 simultaneously checks the **SoD Policy Repository** via a "**SoD Rule Check**" flow.

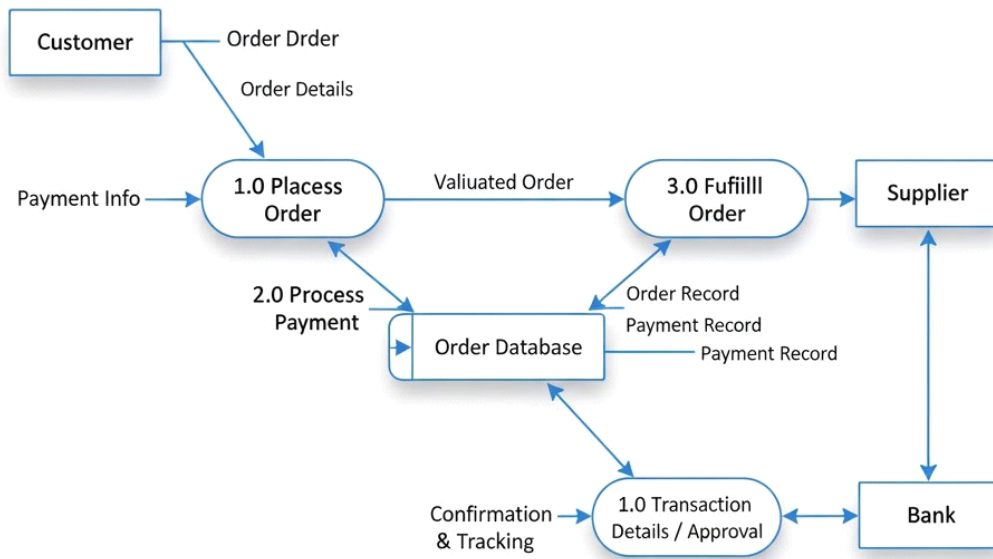
EXAMPLE:

Optimizing User, Group, and Role Management Data Flow (DFD Level 1)

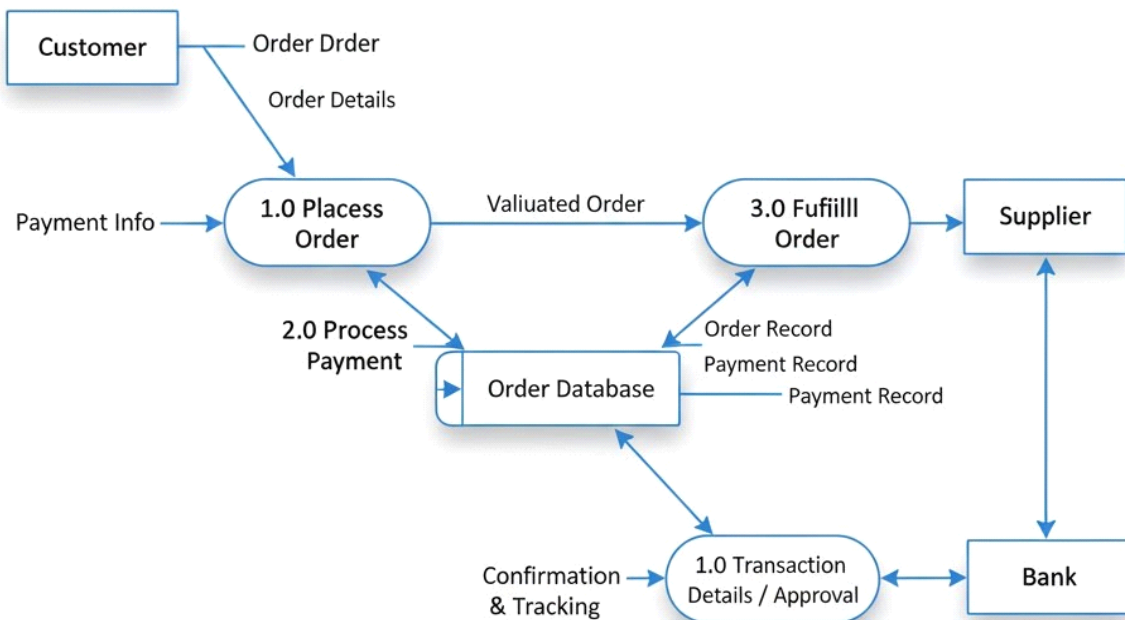


- **Order Initiation:** The **Customer** sends "**Order Details**" and "**Order Order**" (likely "Order Number") to **Process 1.0 (Place Order)**.
○
- **Data Storage:** The **Order Database** is central, storing the "**Order Record**" and "**Payment Record**" from the various processes.
- The database sends "**Confirmation & Tracking**" data back through the system (though the flow from the database isn't fully connected to an external entity, implying a detail is missing or simplified).

Online Ordering System



Online Ordering System



FLOW:

- **Trigger:** Inbound integration (e.g., from HRIS) detects a new user record.
- **Action:** Evaluates existing group memberships and roles to see if the change necessitates adding or removing access (e.g., a move from IT to Finance triggers removal of ITIL roles).

- **Automatically removes the invalid role/membership and generates a report or task for the Administrator.**

User Stories:

- The request must be initiated from a Service Catalog Item titled "Request Fulfillment Role."
- The workflow must first route the request to the Requester's Manager for approval.
- Upon Manager approval, the workflow must check the Separation of Duties (SoD) Policy for conflicts.
- If no conflicts are found, the workflow must automatically add the agent to the designated Group .
- The agent must inherit the `initial` role immediately upon successful group membership.
- The agent must receive an email notification confirming their new access and group membership.

Governance	ParameterDefinition Recommended Value /	FrequencyServiceNow	Implementation Method
Principle Enforced	Least Privilege (PoLP)	Strict adherence across all assignments	Enforced by ACLs and Group-Based Role Assignment.
Access Recertification	Manager reviews and confirms a user's access is still necessary.	Quarterly (High-Risk/Admin Roles) or Bi-annually (Standard Roles)	Flow Designer automation generating Approval/Review Tasks.
Separation of Duties (SoD) Check	Prevents granting two conflicting roles to the same user.	Real-Time during Request Fulfillment	GRC Module integration or custom Script Include logic in the workflow.