Project Design Phase: Solution Architecture

Field	Detail
Date	**02 November 2025**
Team ID	**NM2025TMID00414**
Project Name	**Optimizing User Group and Role Management with Assess, Control, and Workflow**
Maximum Marks	**4 Marks**

Solution Architecture

Goals of the Architecture

- **Establish a Centralized Access Governance Platform** to unify user, group, and role data.
- **Enforce the Principle of Least Privilege** by mandating all access assignments and changes flow through auditable workflows.
- **Automate Access Recertification (Assess)** to ensure roles are periodically validated and de-provisioned if no longer needed.
- **Maintain Compliance and Audit Readiness** by recording every access decision and change in a comprehensive log.

Key Components

- **Identity Repository (e.g., Active Directory/LDAP, HCM System):** The single source of truth for all users.
- **Role Management Engine (Control):** A service that defines, stores, and manages the static set of approved organizational roles (e.g., RBAC model).
- **Workflow & Approval Engine (Workflow):** A component that processes all access requests (add, modify, delete) and triggers multi-stage approvals, and performs automated risk/SoD checks.
- **Access Recertification Module (Assess):** A scheduled service that initiates periodic reviews of all current role assignments.
- **Provisioning Connector:** Integrates with target systems (e.g., SaaS apps, databases) to automatically execute access changes approved by the Workflow Engine.

Development Phases

1. **Phase 1: RBAC Model Design:** Define the initial set of business roles and map them to necessary technical permissions within a sandbox environment.
2. **Phase 2: Workflow Engine Setup:** Configure the access request, approval, and recertification workflows based on pre-defined policies (e.g., Manager Approval, SoD Checks).
3. **Phase 3: Integration & Testing:** Establish connectors between the Identity Repository, Workflow Engine, and a target application (e.g., a test instance of an ERP or CRM).
4. **Phase 4: Pilot Rollout & Assessment:** Onboard a small user group, perform a full access recertification cycle, and measure metrics like time-to-provision and audit failure reduction.

Solution Architecture Description

The solution architecture is designed to implement a holistic **Identity Governance and Administration (IGA)** framework focused on the Assess, Control, and Workflow pillars. A central **Role Management Engine** serves as the core, defining standardized roles (Control). All user access changes must be initiated via the **Workflow & Approval Engine**, which applies configured access policies and automatically routes requests to the appropriate approvers (Workflow). Critically, a dedicated **Access Recertification Module** (Assess) runs on a scheduled basis, systematically presenting current access lists to managers or role owners for validation, ensuring that privileges are automatically revoked if unapproved. The entire process is linked via **Provisioning Connectors** to target applications, ensuring that policy decisions are executed reliably and instantly across the enterprise.

Example - Solution Architecture Diagram

This diagram illustrates the logical flow:

1. **User Identity:** HR/AD feeds user data to the **Identity Repository**.
2. **Request:** A user or manager submits an access request to the **Workflow Engine**.
3. **Control/Assess Logic:** The Workflow Engine checks the request against the **Role Management Engine** (RBAC rules) and triggers **Recertification Module** checks.
4. **Approval:** If approved, the request is sent to the **Provisioning Connector**.
5. **Provisioning:** The connector executes the change on the **Target Application** (e.g., grants membership to a specific User Group).
6. **Audit:** All events are logged in the **Audit Repository**.