Project Design Phase-IV: Technical 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

Technical Architecture

The architecture will adopt a **Microservices-based** approach to ensure **scalability, high availability, and loose coupling** between the core governance functions (Assess, Control, Workflow) and the target systems. The core platform will serve as an **Identity Governance and Administration (IGA)** layer that sits between the HR/Identity source and the final enterprise applications.

- **Layer 1: Presentation Layer:** Self-Service Portal and Admin Dashboard for user interaction.
- **Layer 2: Core Governance Layer (Microservices):** Separate services for **Role Engine (Control)**, **Workflow Engine**, and **Recertification Engine (Assess)**.
- **Layer 3: Data Layer:** Highly available database for storing user, role, policy, and audit data.
- **Layer 4: Integration Layer:** Standardized **Provisioning Connectors** (e.g., SCIM, API integration) for communication with target systems.

Components and Technology

S.No.	Component/Tool	Description
1.	**Identity Source Integration**	**Technology:** LDAP/Active Directory, SCIM 2.0, or HR System API Connector (e.g., Workday API).
2.	**Role Management Engine (Control)**	**Technology: Java Spring Boot Microservice** or **Python-based service**. Manages role definition, entitlements, and the RBAC policy enforcement logic.
3.	**Workflow Engine**	**Technology: Camunda or Activiti** (BPMN engine). Manages the sequential flow, approval routing, and policy checks (e.g., SoD).
4.	**Access Recertification Engine (Assess)**	**Technology:** Scheduled service running on **Kubernetes/AWS Lambda**. Triggers review campaigns and manages email notifications

S.No.	Component/Tool	Description
		and access revocation.
5.	**Data Store**	**Technology:** Highly available **PostgreSQL or MongoDB** (for audit logs). Stores policy data and immutable audit trails.
6.	**Provisioning Connector**	**Technology: SCIM Gateway** or custom API wrappers. Acts as the interface to provision/deprovision access on systems like SAP, Salesforce, etc.

Application Characteristics

S.No.	Characteristic	Description
1.	**Interoperability**	Must integrate via **SCIM** and native APIs with at least **three major target systems** (e.g., HR, ERP, Cloud Provider) to ensure broad access control.
2.	**Scalability**	Must be horizontally scalable to support managing **over 100,000 identities** and processing **1,000 approval requests per hour** during peak load.
3.	**Security**	Requires **end-to-end encryption** for data at rest and in transit, and must enforce **Role-Based Access Control (RBAC)** even for its own administrative interface.
4.	**Maintainability**	The use of standardized microservices and a recognized workflow engine (BPMN) ensures the system can be easily updated and customized without disrupting core functionality.