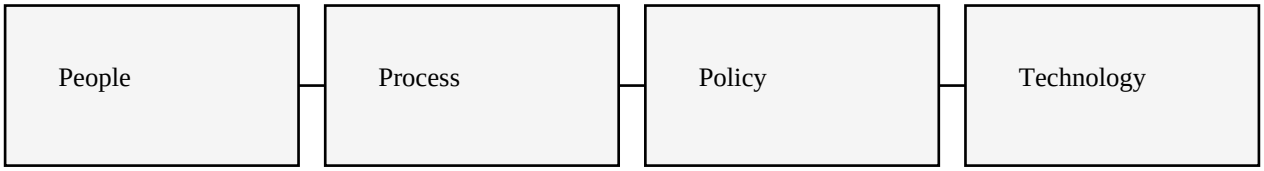
Define Problem Statement

Project: Optimizing User, Group, and Role Management with Access Control and Automated Workflows

Enterprises handling identity & access face significant complexity. Current IAM implementations across typical enterprise SaaS platforms experience heavy manual intervention, operational overhead, misaligned permissions, delayed approvals, and compliance exposure. Business scale multiplies this problem because every new user, group, role or permission combination increases risk exponentially when workflows are manual.

Problem Factor	Current State	Enterprise Impact
Role Assignment	Manual mapping of each user to roles	Slow provisioning / onboarding delay + error risk
Access Enforcement	No centralized rules enforcement	High chance of privilege escalation
Group Management	Department segregation happens manually	Operational friction & inconsistency
Audit History	Limited visibility & no identity lineage	Compliance & SOC2 failure possibility
Multi-Approval Flows	Not available	Breaks org security governance policy
Access Revocation	Offboarding is delayed	Stale access risk & threat persistence
Data Traceability	Multiple disconnected access systems	Cannot maintain single source of truth
Policy Enforcement	Admin interpretation dependent	Security depends on human decisions (danger)

T2 Enterprise SaaS IAM Context Visualization



Conclusion Need Statement

Enterprises require a fully governed IAM operating model where identity based security is not manually controlled but automated, validated, version tracked and workflow driven. This project delivers a central platform where User, Group and Role mapping happens with frictionless automated workflows, strict access guardrails, lifecycle traceability, multi-approval gates and least privilege enforcement. This eliminates uncertainty, risk, delays and transforms IAM into predictable and auditable enterprise governance architecture.