## Proposed Solution - Optimizing User, Group, and Role Management with Access Control & Automated Workflows

• Establish a Zero Trust based RBAC + ABAC hybrid identity model across all cloud and on-prem IAM engines.

• Automate workflow driven approval paths for new users onboarding, role elevation, group mapping & revocation.

• Introduce a central attribute inference engine to map identity attributes → groups → roles automatically.

• Apply continuous audit intelligence with event lineage trace to prevent misconfigured privilege grants.

• Make policy decisions data-driven using identity risk signals, user behavior analysis and historical access maps.

## Architecture Diagram 1 (Style C)

USER → APP → CLOUD IAM → ROLE ENGINE → POLICY ENFORCEMENT → ZERO TRUST DECISION

| Capability | Benefit |
|---|---|
| Automated Role Mapping | Reduces manual admin burden & error |
| Workflow Driven Approvals | Faster onboarding & audit visibility |
| Risk Adaptive IAM | Prevents privilege misuse & policy drift |

## Architecture Diagram 2 (Style C - Cloud Zero Trust)

IDENTITY ATTRIBUTES → NORMALIZATION ENGINE → ROLE INFERENCE ENGINE → POLICY VALIDATION ENGINE → ACCESS ENFORCEMENT ENGINE

## Final Solution Summary

The proposed automated IAM architecture ensures stable policy enforcement, scalable role governance, cross cloud consistency and end-to-end privilege lifecycle automation with measurable governance maturity uplift.