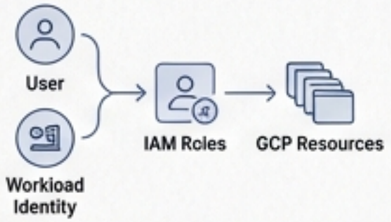
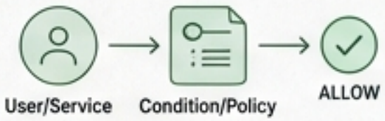
Google Cloud Professional Security Engineer

Section 1 Mastery: Configuring Access & Governance

IDENTITY & ACTORS

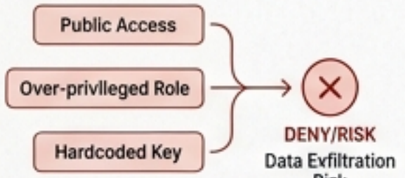


AUTHORIZATION & ALLOW

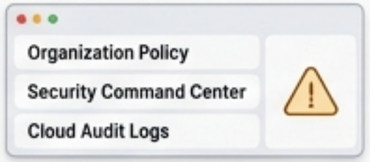



```
gcloud projects add-iam-policy-binding
```

DENY, RISKS, ANTI-PATTERNS

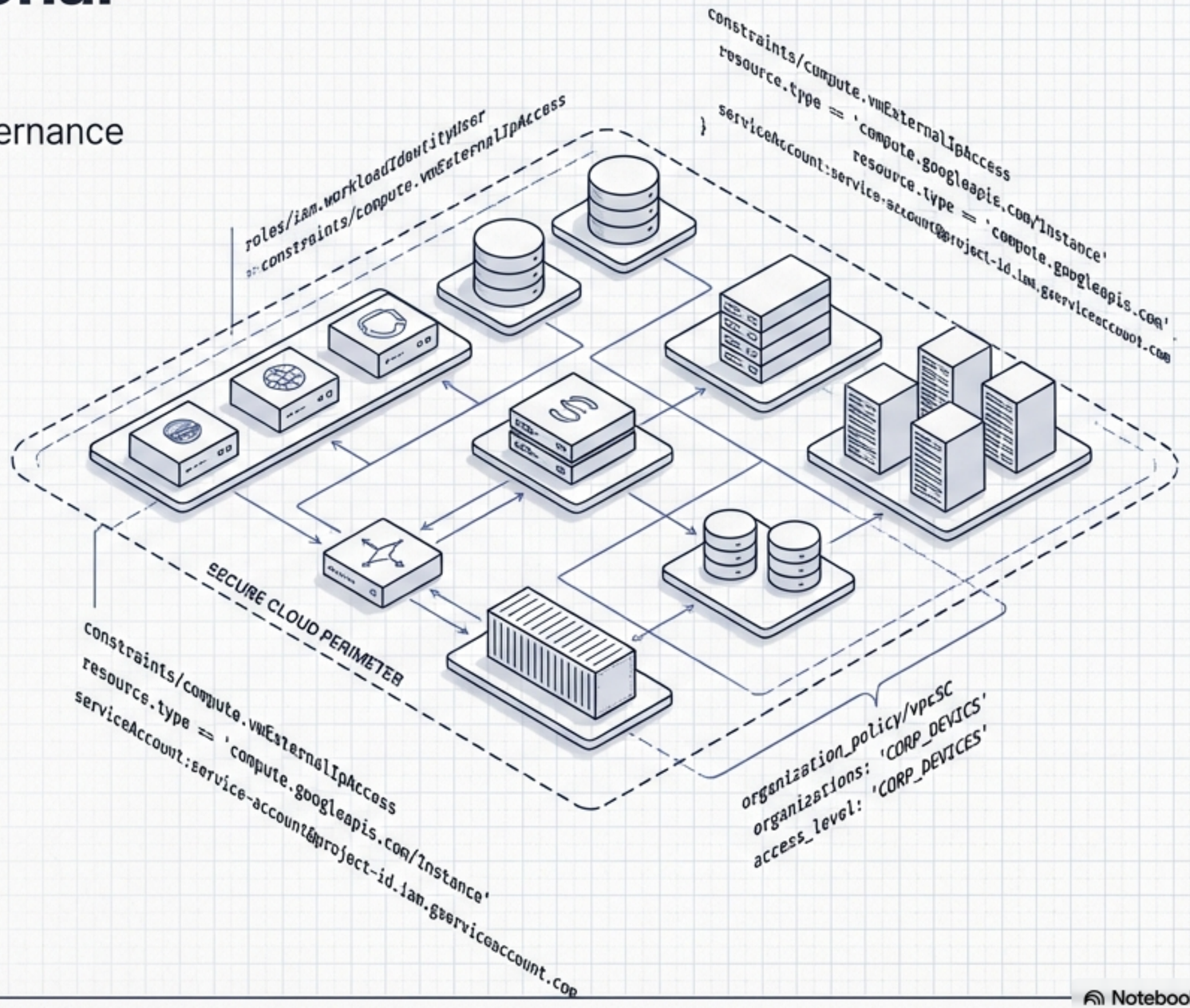


ALERTS & POLICIES




```
alert_type: 'IAM_POLICY_CHANGE'
```

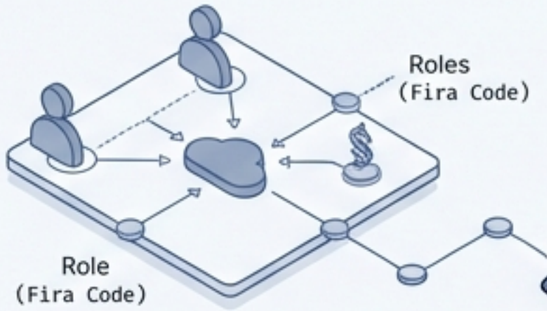
A Visual Guide to Access, Identity, and Governance



Access is an equation of **identity**, **context**, **permissions**, and **boundaries.**

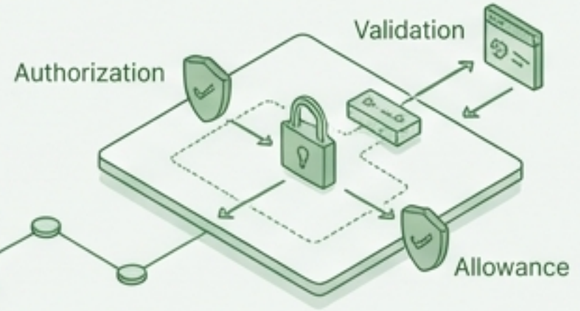
Who
Human Actors

Cloud Identity, GCDS, Workforce Federation



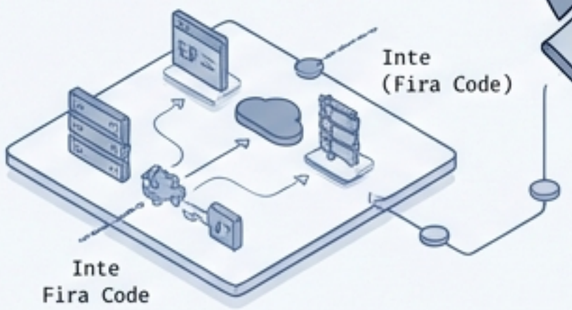
How
The Gates

Authentication, IAP, IAM, Privileged Access Manager



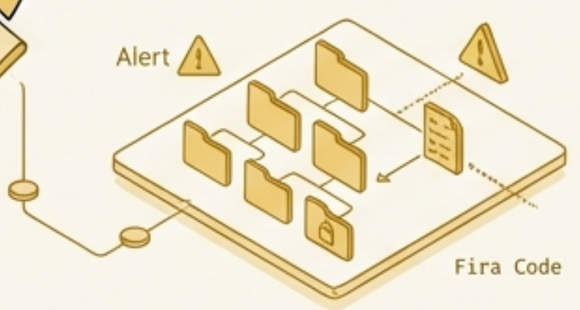
What
Machine Actors

Service Accounts, Workload Identity



Where
The Boundaries

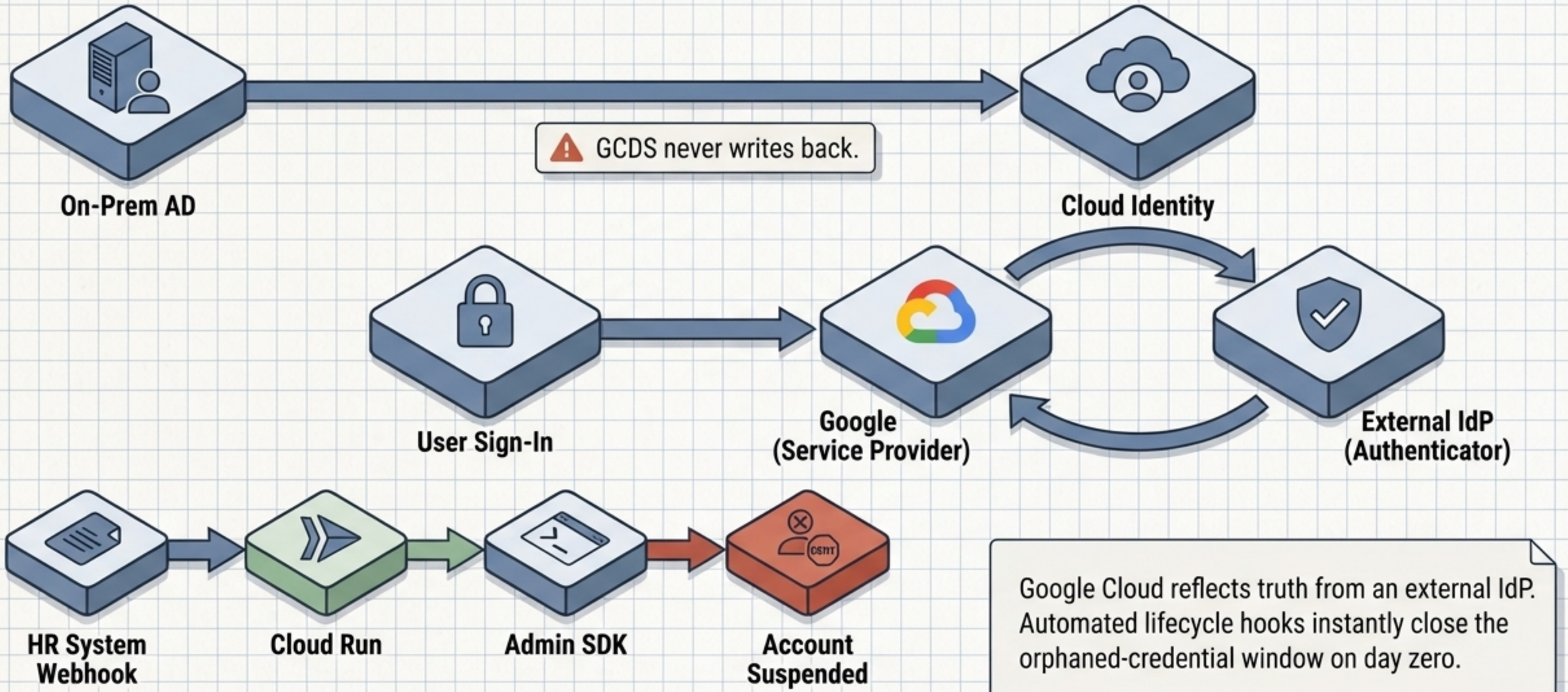
Resource Hierarchy, Organization Policies



True cloud security requires interlocking all four quadrants. Manipulating just one component leaves the architecture vulnerable.

Synchronizing external human identity into Google Cloud.

This Daylight Blueprint style ats Inter, body text. Inter Light, ɱmtrization and technical terms in `Fira Code`.



Google Cloud reflects truth from an external IdP. Automated lifecycle hooks instantly close the orphaned-credential window on day zero.

Super Admin accounts require absolute, uncompromising security constraints.

Security Command Panel

Hardware Keys Only (FIDO2/Titan)

The only 2SV method that defeats real-time phishing.

No Day-to-Day Use

Strictly reserved for organizational recovery and top-level governance.

Minimum Two Break-Glass Accounts

Maintained offline to ensure redundancy during lockouts.

Zero Application Credentials

No associated OAuth tokens or application-specific passwords permitted.

Eliminating standing credentials through identity federation.

Workforce Identity Federation

	Target: Human contractors and temporary employees.
	Mechanism: External IdP (`OIDC/SAML`) directly mapped to GCP.
	Advantage: Grants access to Google Cloud resources without synchronizing directories or creating user accounts in Cloud Identity.

Workload Identity Federation

	Target: External machines (`GitHub Actions`, `AWS Lambda`).
	Mechanism: External platform `OIDC/SAML` mapped to GCP.
	Advantage: Replaces the need to export, store, and manually rotate persistent JSON service account keys.

Key Takeaway: Both frameworks rely on **short-lived, external trust** to eliminate standing accounts and persistent keys within Google Cloud.

Migrating machine access from persistent keys to transient tokens.

RISK SPECTRUM

1

Long-Lived JSON Keys

Stored on laptops, high blast radius

Mitigation: Audit >90 days unused, use `constraints/iam.disableServiceAccountKeyCreation`

2

Default Compute SA

Broad editor roles automatically granted to the environment.

Mitigation: Block automatic grants via Org Policy.

3

SA Impersonation

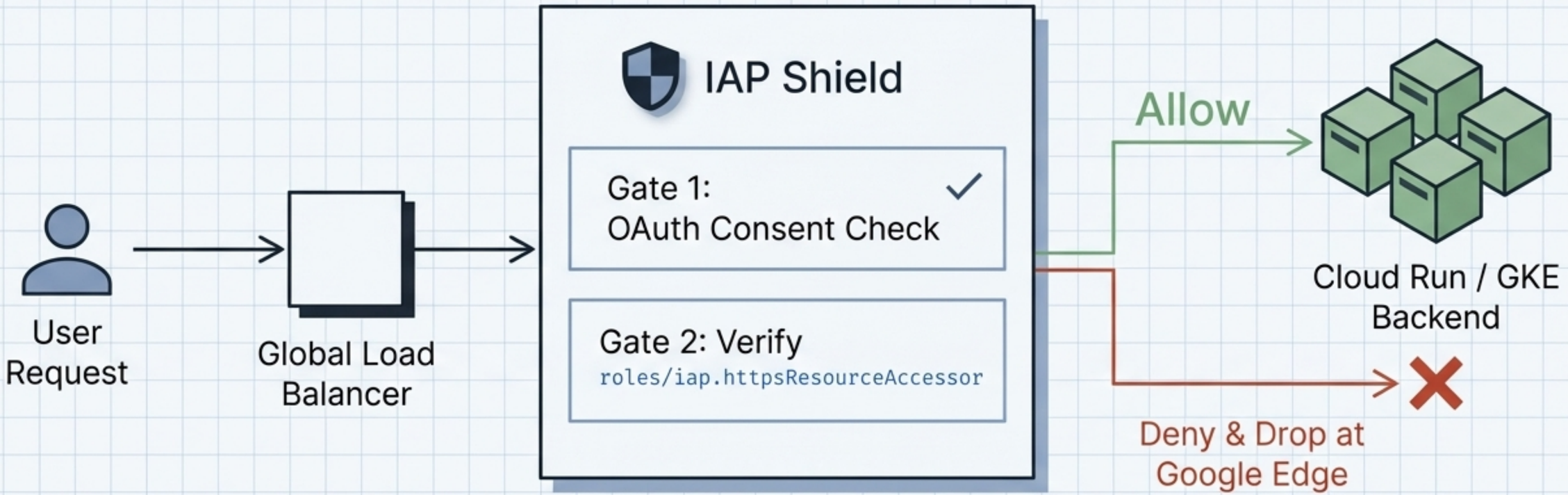
Short-lived OAuth tokens via `generateAccessToken` using `roles/iam.serviceAccountTokenCreator`

4

Workload Identity

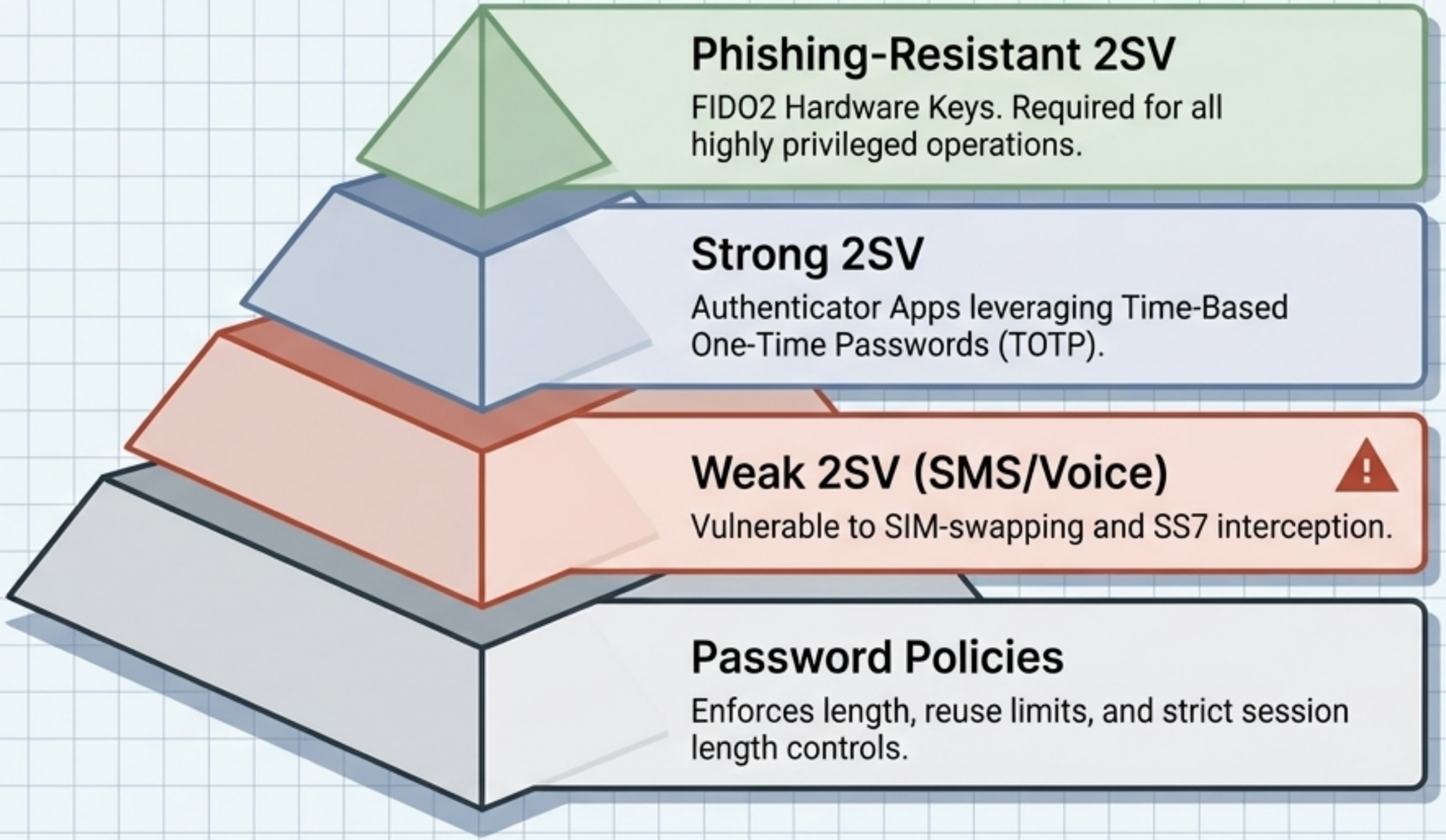
GKE and Cloud Run auto-rotated metadata tokens. Zero key management required.

Identity-Aware Proxy enforces zero-trust verification at the network edge.



IAP drops the VPN requirement entirely. Access can be revoked in seconds by updating Google Group memberships, terminating the connection before it reaches the backend.

Authentication strength must scale with account privilege.

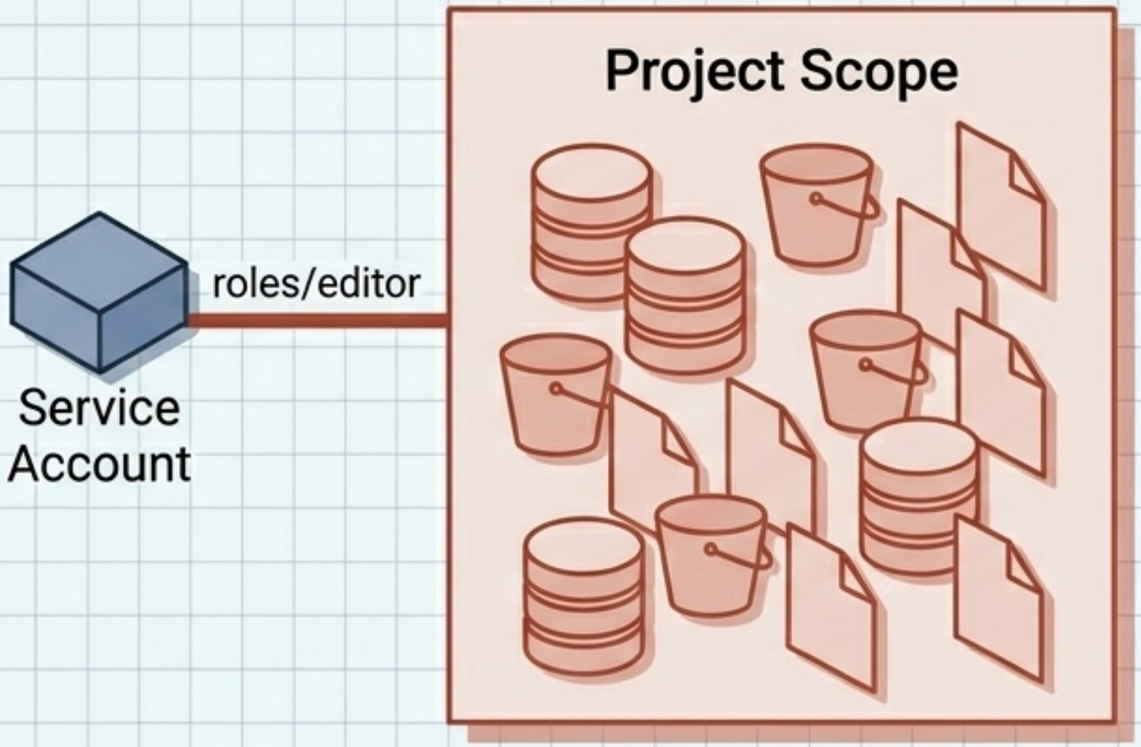


SAML Context

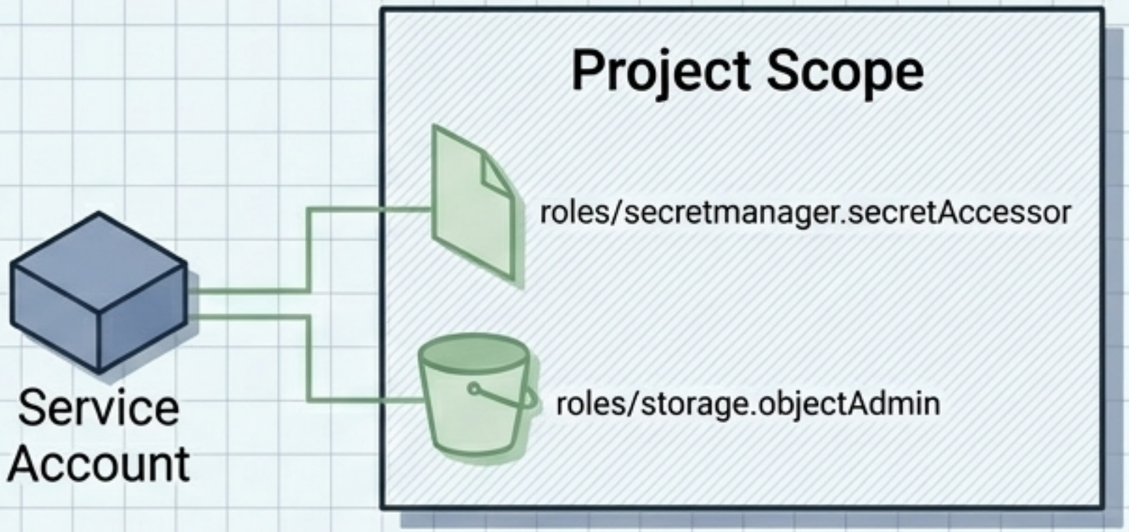
When Google acts as the Identity Provider for third-party applications, it securely asserts these authentication attributes to the Service Provider via a signed SAML assertion.

Least privilege demands resource-level, not project-level, bindings.

✗ Anti-Pattern



✓ Target Architecture



Uniform Bucket-Level Access must be enabled to prevent legacy per-object ACLs from overriding this strict IAM policy.

Context and explicit denials override standard allow policies.

IAM Conditions (ABAC)

```
request.time < 17:00:00
```

```
resource.name ==
'projects/prd'
```

Restricts access by specific time bounds (business hours), IP origin, or targeted resource names.

Access Context Manager

Device Trust IP Origin Geolocation

Feeds zero-trust state directly into VPC Service Controls and IAP.

IAM Deny

Evaluated absolutely first. Blocks actions universally, successfully overriding even Project Owners.

Example: Preventing audit log disablement.

EVALUATED FIRST, OVERRIDES ALLOWS

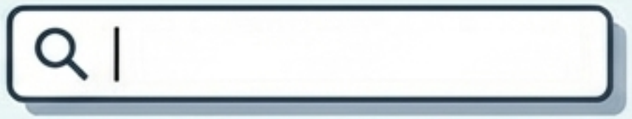
Policy intelligence and Just-In-Time access eliminate standing privileges.

Recommender

90-day usage analysis

Identifies and revokes roles that were granted but left unused.

Analyzer



Queries “Who has access to Resource X?” instantly across the entire organization.

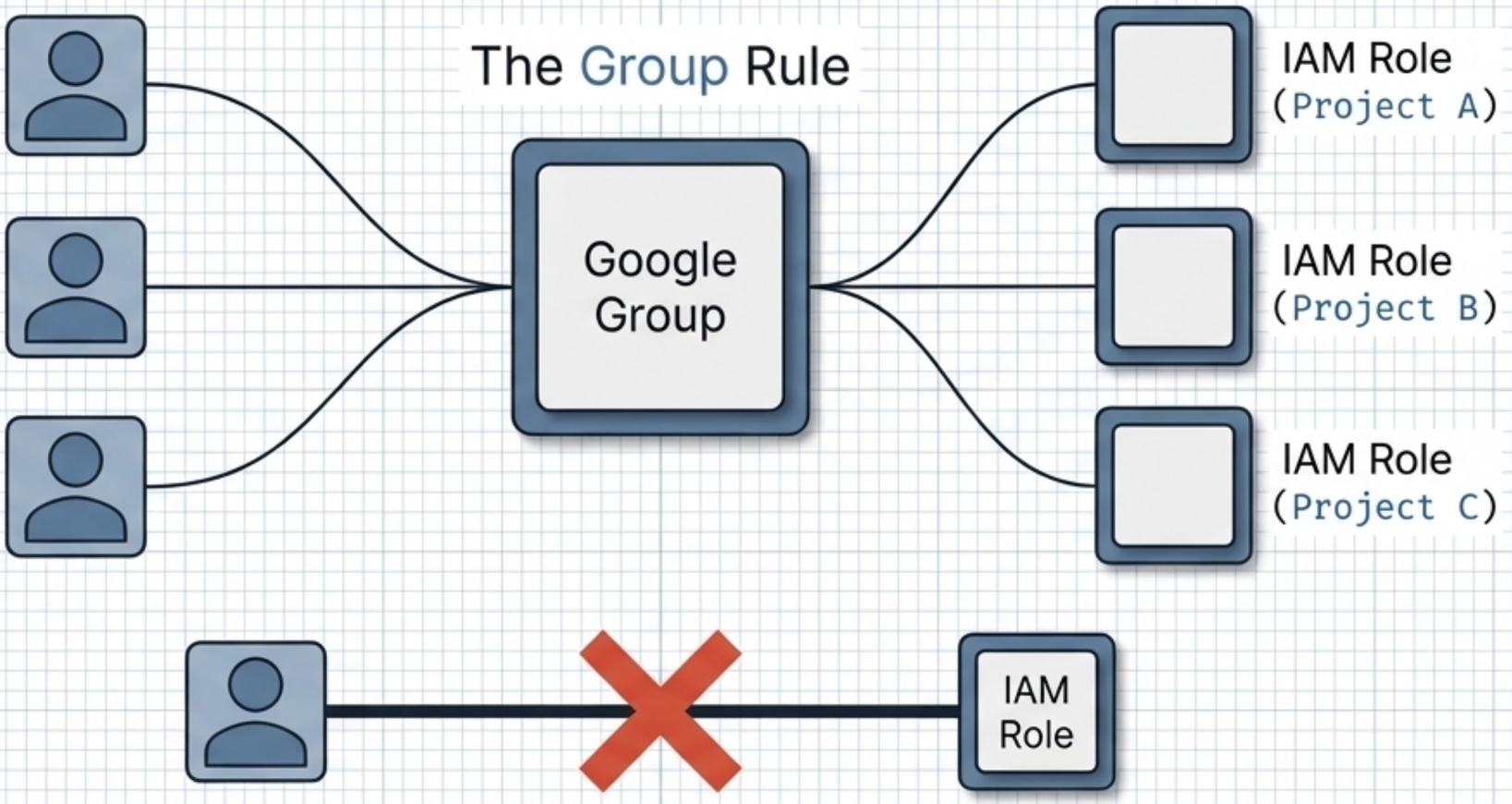
Troubleshooter

Traces policies to explain exactly why a specific permission was allowed or denied.

Privileged Access Manager (PAM)

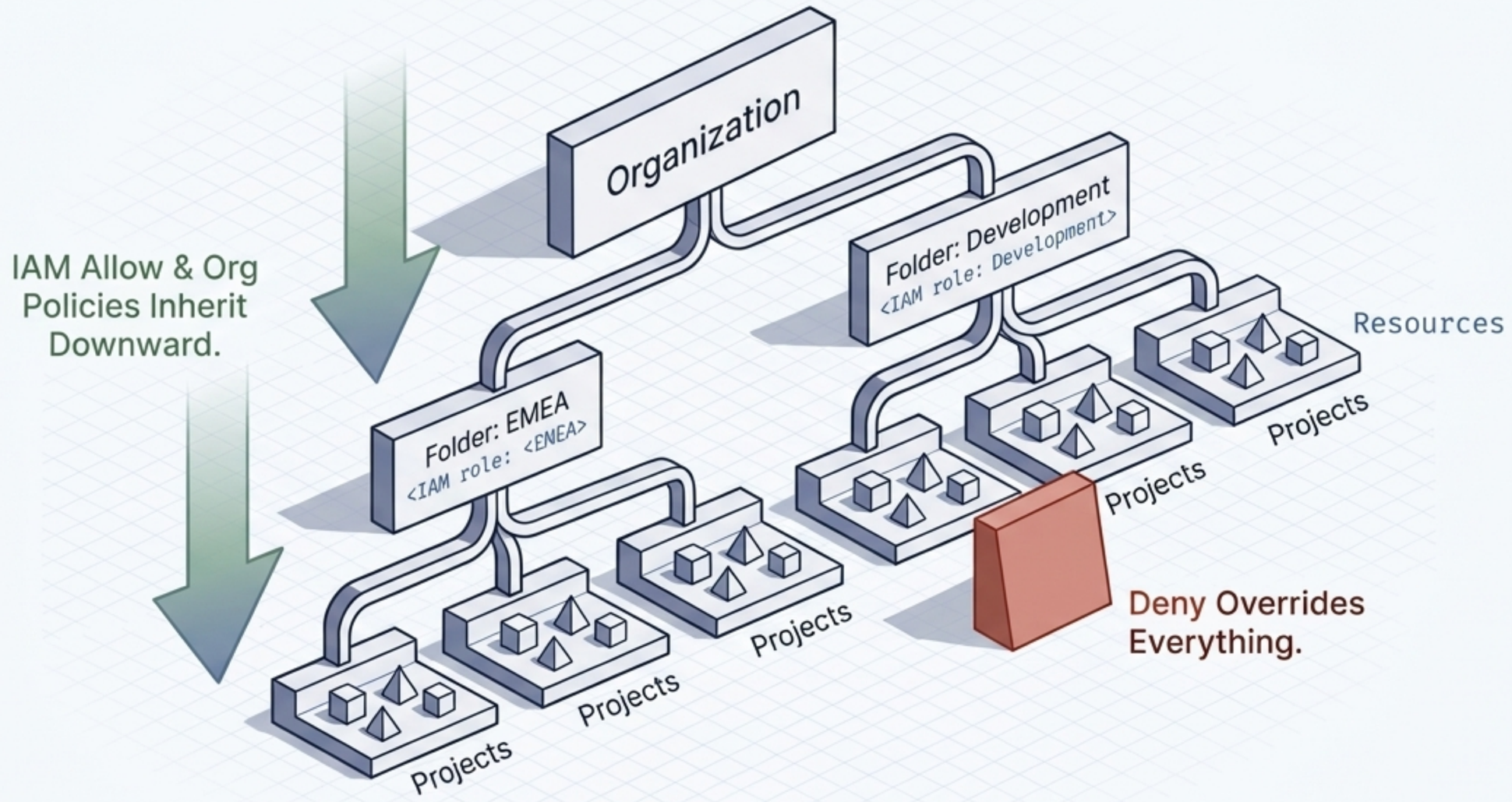
Request → Justification → Approval → Temporary Role Granted → Auto-Expiry + Audit Log

Scaling permission management through Google Groups.



Never attach IAM policies to individual users. Adding a user to a group yields instant, atomic access provisioning. Removing them yields instant, global revocation across all Google Cloud resources.

Security constraints cascade downward through the resource hierarchy.



A developer cannot bypass an organization or folder constraint by modifying a local project's settings. Governance flows from the top.

Organization policies secure the environment before resources are created.

Command Console

Built-in Defenses

`constraints/compute.vmExternalIpAccess`
(Blocks external IPs)

`constraints/gcp.resourceLocations`
(Restricts to specific regions, e.g., EU-only)

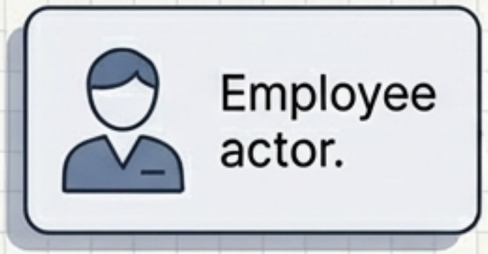
`constraints/iam.disableServiceAccountKeyCreation`
(Blocks all new SA keys)

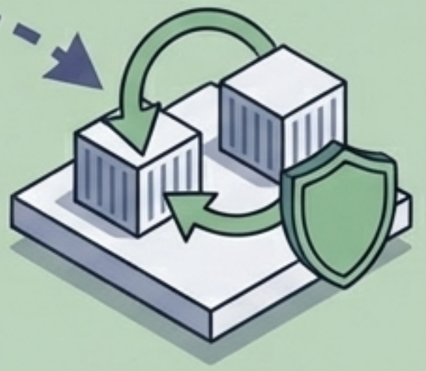
Custom Constraints

```
condition: resource.settings.ipv4Enabled == false
action: DENY
```

CEL rule explicitly blocking the creation of a Cloud SQL instance if it lacks a private IP.

A properly configured environment automates security through the entire lifecycle.





1. Employee departs.

On-Prem Active Directory is immediately disabled.

2. GCDS Sync.

One-way sync executes; Cloud Identity account is suspended.

3. Atomic Revocation.

Group membership drops, instantly terminating IAM bindings and IAP edge access across the entire organization.

4. Workload Continuity.

Underlying deployed container workloads continue running safely via Workload Identity, completely unaffected by human departure.

When identity, authorization, and hierarchy are properly mapped, zero manual cloud intervention is required when human status changes.