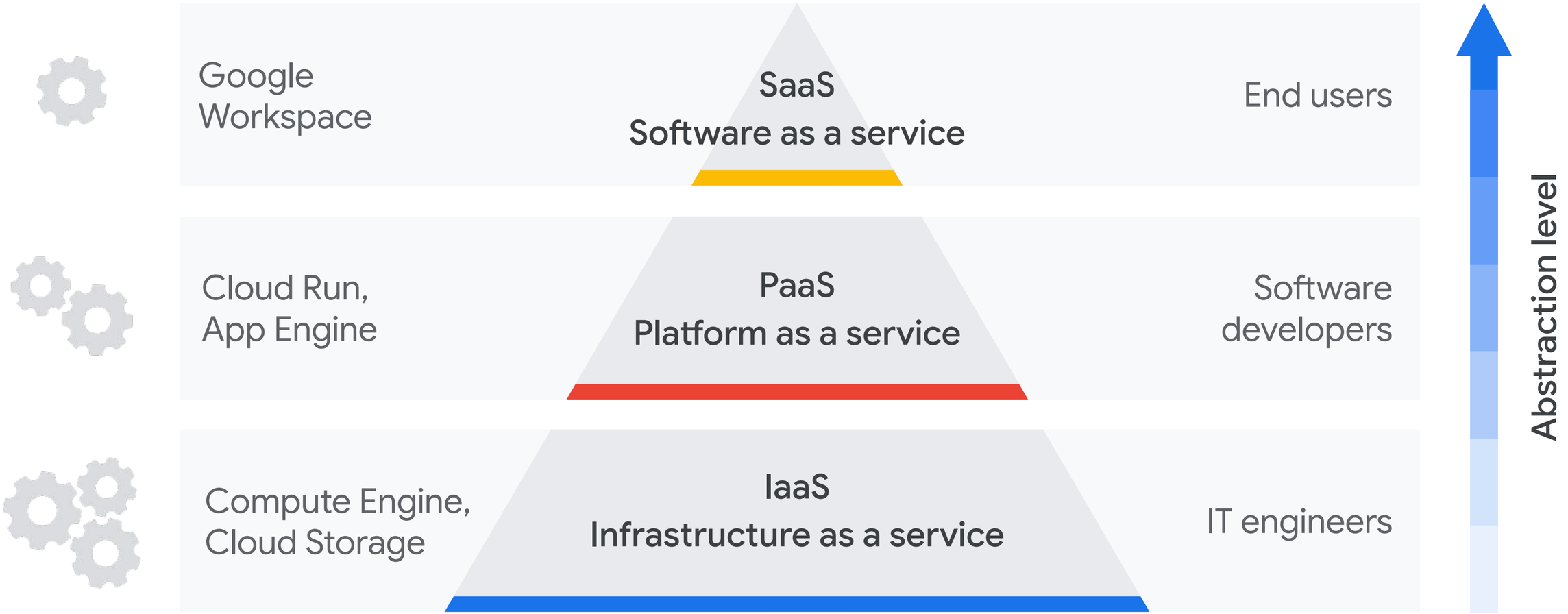
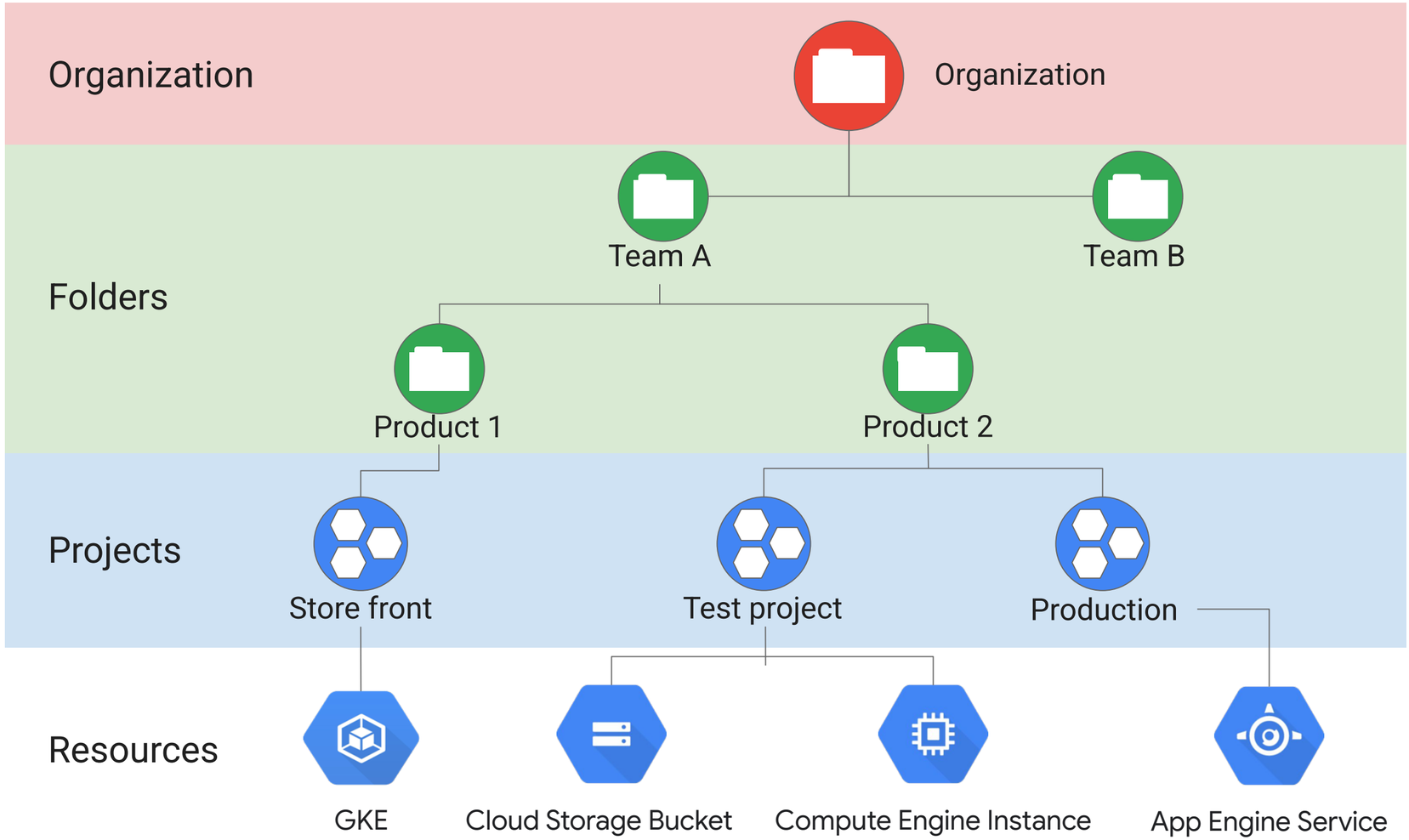
Abstraction hides underlying infrastructure



Resources have hierarchy



Exam Tip: *Privileges always propagate down = The effective policy for a resource is the union of the policy set at that resource and the policy inherited from its parent (not true anymore from 03.2022 when Deny policies were introduced, but exam is not yet "aware" of it).*
BUT: Organizational Policies (eg. restriction that only resources in some regions can be created) CAN be overwritten on lower levels

Cloud Identity vs IAM

Cloud Identity	IAM
Identity as a Service (IDaaS) solution that centrally manages users and groups. Often configured to federate identities between Google and other identity providers (AD etc).	Service that lets authorize who can take action on specific GCP resources
In Cloud Identity, you manage BOTH identities AND privileges (via roles). However, it's NOT GCP-specific...	With IAM, you manage privileges (via roles) only. Identities need to be created in advance, in most cases: in Cloud Identity (with the exception of Service Accounts).
Most important role: Super Admin (full access and manage other Admins). Needed to configure GCP organization (= grant Oganization Administrator role to others). NOT for daily use. Should use MFA	Most important role: Organization Administrator. Designed to manage day to day organization operations in GCP (= mostly grant IAM roles to identities).
Has a Free and Premium editions, each with different features.	

Exam Tips:

- *Make sure to differentiate and know best practices of Super Admin (Cloud Identity role) vs Organization Administrator (IAM Role)*
- *If you'd like to know how to create new GCP organization, see this guide.*

Identity and Access Management (Authentication)

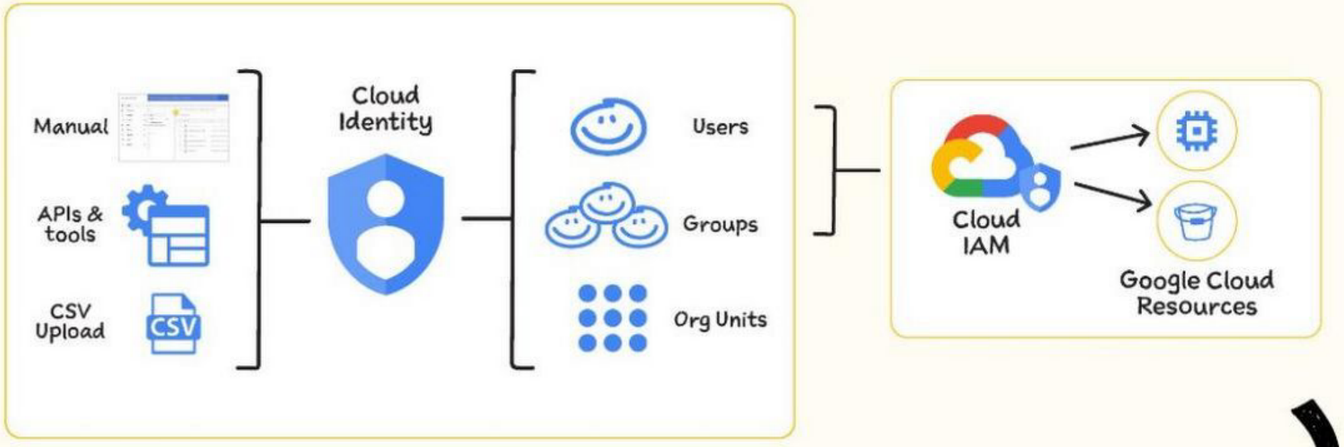
#GCPSketchnote @PVERGADIA THECLOUDGIRL.DEV 11.10.2021

How do you control user access?

AUTHENTICATION — Cloud Identity

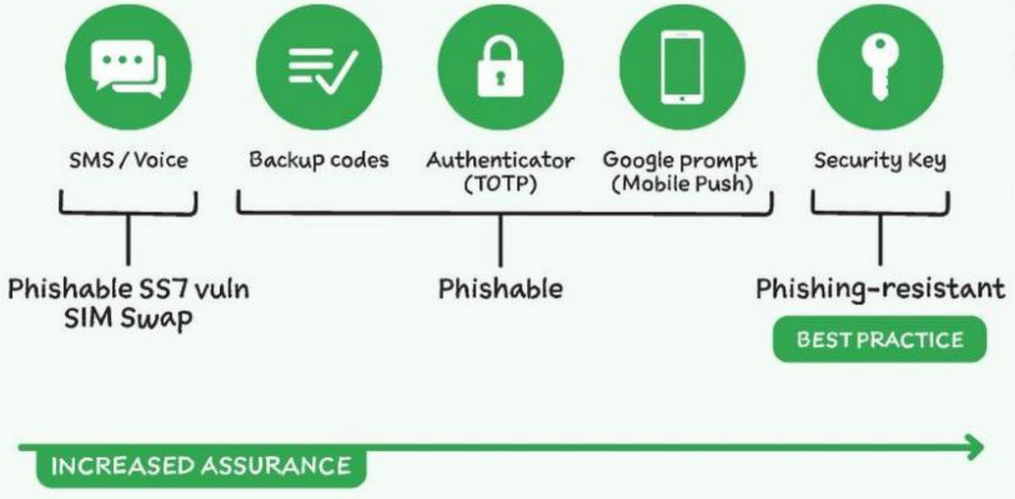
AUTHORIZATION — Cloud IAM

WHAT IS CLOUD IDENTITY (AUTHENTICATION)?

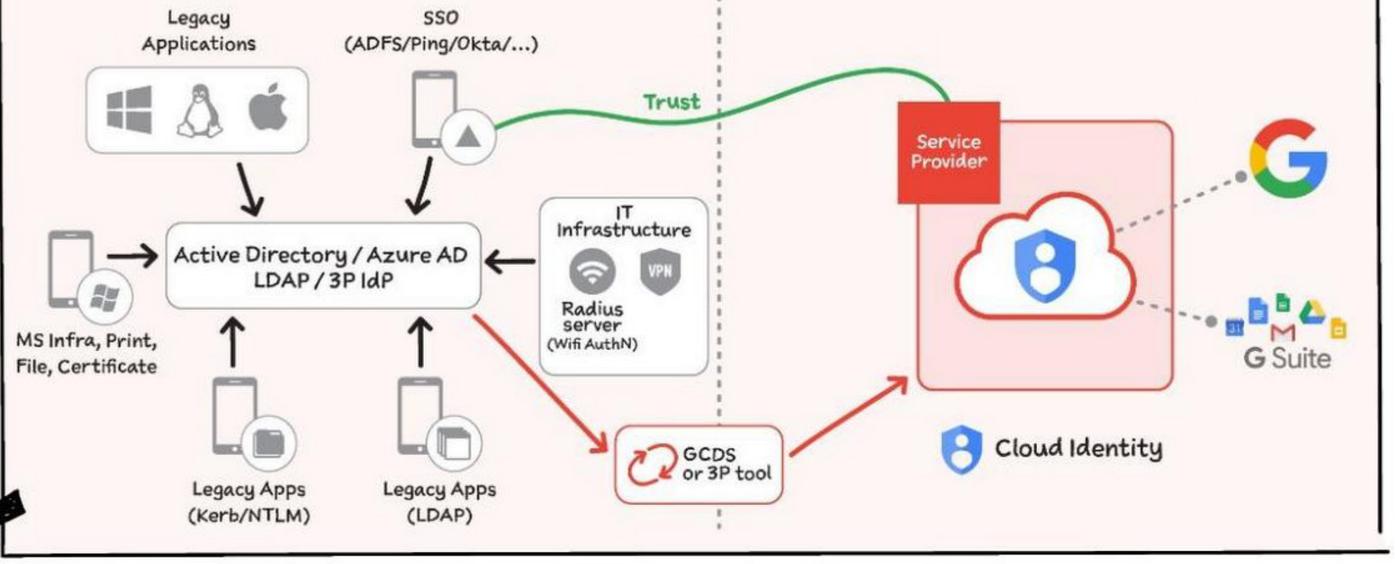


2SV WITH GOOGLE AUTHENTICATION

Any 2SV is better than no 2SV, but not all the 2SV methods are the same



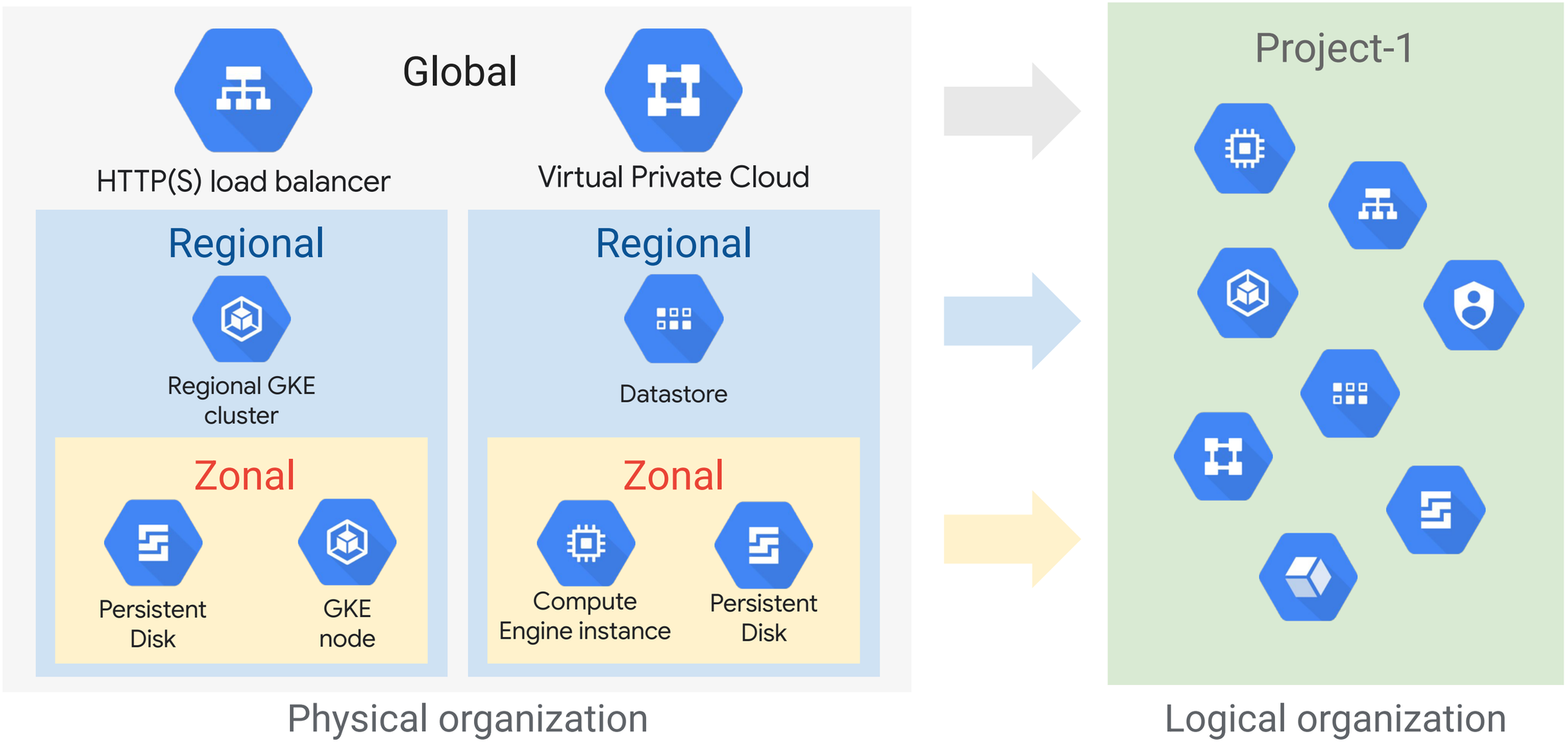
THIRD-PARTY AS AN IDENTITY PROVIDER: TYPICAL ARCHITECTURE



Organization Policy vs IAM Policy

Organization Policies	IAM Policies
Constraints that allow you to: • Limit resource sharing based on domain. • Limit the usage of Identity and Access Management service accounts. • Restrict the physical location of newly created resources.	Effectively they're bindings which specify what access should be granted to principal on resources.
Focuses on "what". Allows to set restrictions on specific resources to determine how they can be configured	Focuses on "who". Let's you authorize who can take action on specific resources based on permissions
Can be set on different levels (org, folder, project), propagate down but lower-level policy overwrites a higher-level one.	Effective IAM Policy on each level is a SUM of all privileges (* with an exception of "deny policies", which are not covered on the exam as of Q1 '23)
Both should be used as part of a security posture! It's NOT one or the other.	

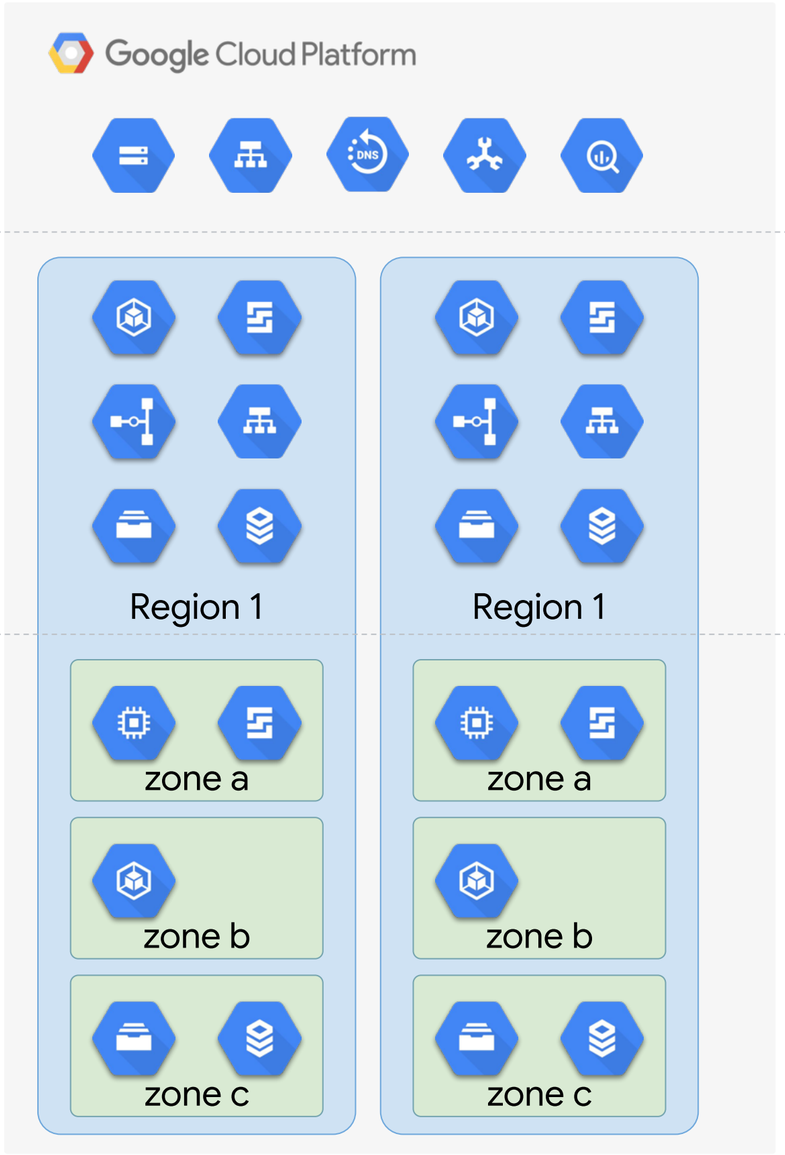
Resources are organized both physically and logically



Exam Tip: *Know on which physical level (zone / region / multi-region / global) each service lives in.*

Physical distribution of GCP resources

- Not all services provide regional availability, and not all regional services are made equal. Regional deploy may have RTO & RPO > 0 (e.g.: minutes for regional Cloud SQL).
- DNS updates may take longer than expected (TTL, caching).
- Restoring a VM from a snapshot gives you a new VM with a different IP, by default.
- When using multi-regional deployments, beware of split-brain issues.



Multi-regional

- Cloud Storage
- Cloud Load Balancing
- Cloud DNS
- Spanner
- BigQuery

Regional

- Google Kubernetes Engine (regional)
- Regional Persistent Disk
- VPN & Interconnect
- Cloud Load Balancing
- Spanner
- Filestore
- Cloud SQL

Zonal

- Compute Engine
- Persistent Disk
- Google Kubernetes Engine
- Filestore
- Cloud SQL

OPTIONAL study materials:

[READING]

- What are IAM Conditions
- get familiar with Migrating to GCP: Getting Started as much as possible

[VIDEOS]

- Cloud Networking 101: Cloud OnAir: Google Cloud Networking 101
- A lot of short overview videos for different GCP services (2019 and before, but mostly still applicable): Cloud Performance Atlas
- **How to start with GCP as an organization** - a unique opportunity to see how to validate & attach a domain to GCP, create an organization and set up Cloud Identity in a recommended, secure way: Level Up From Zero Episode 1: Domains, Identity, and Admin Accounts
- How to design resource hierarchy in GCP: Level Up From Zero Episode 2: Organizations & the Resource Hierarchy
- Creating IAM Policies: Level Up From Zero Episode 3: Identity & Access Management
- How does networking work between GCP data centers: How does networking work across Google's data centers?
- Organizations and resource hierarchy: Level Up From Zero Episode 2: Organizations & the Resource Hierarchy
- IAM: Level Up From Zero Episode 3: Identity & Access Management
- What are Service Accounts?
- Creating, managing, and retiring Service Accounts
- (if you want to understand Resource Hierarchy really well): Best Practices: GCP Resource Organization and Access Management (Cloud Next '19)

OPTIONAL study materials:

[PODCASTS]

- Nice overview of Cloud SDK and CLI
- GCP Cost Optimization
- Cloud Logging

[DEEP DIVES]

- Want to understand IAM policies well? Then it's a must-watch for you: Advanced IAM: Hacks, tips, and tricks for policy management
- Great demo of using and impersonating Service Accounts: Service Accounts in action
- Encryption at rest.
- Encryption in transit.

Make sure to...

Enjoy the journey as much as the destination!