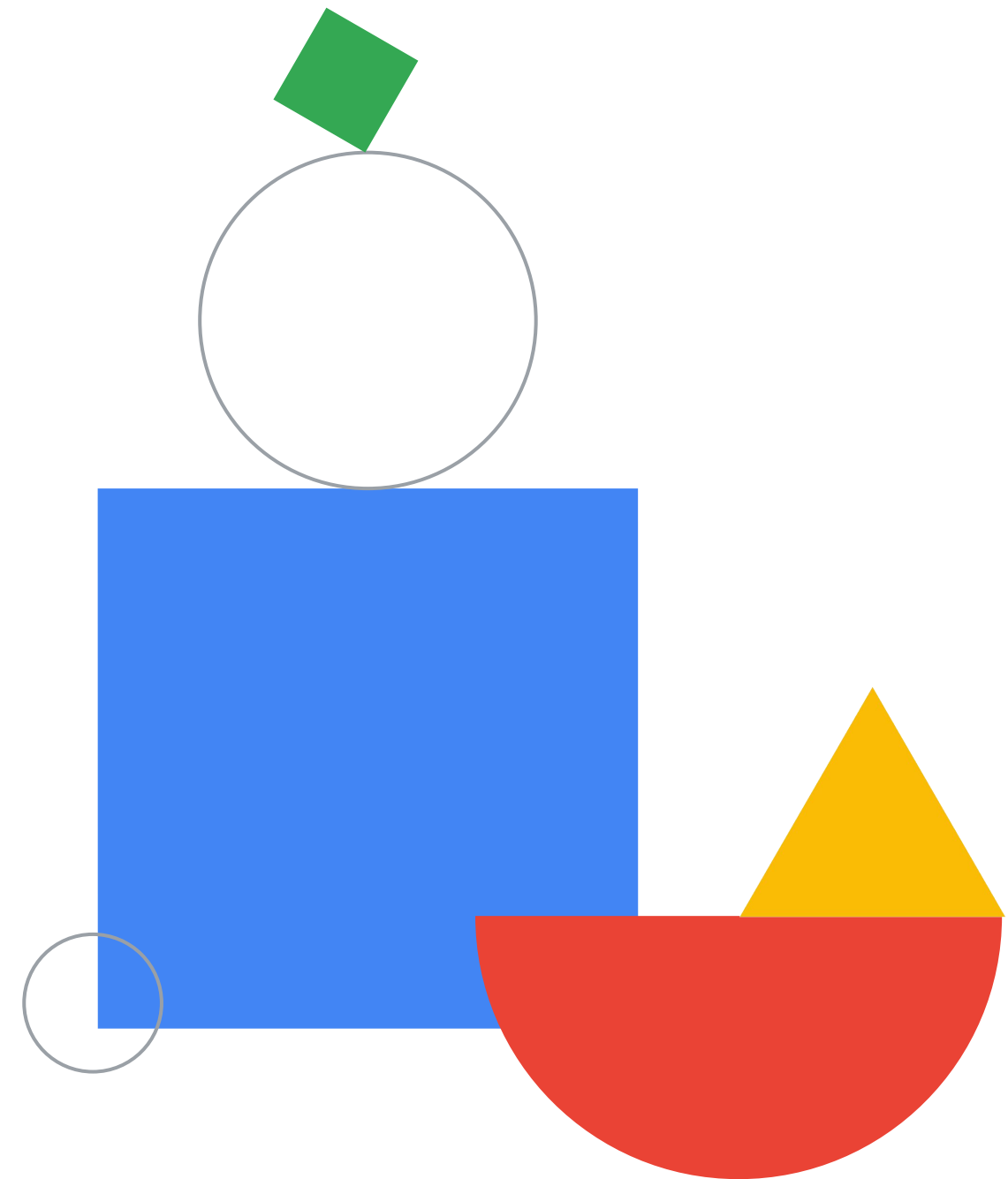


Preparing for Your Professional Cloud Architect Journey

Introduction

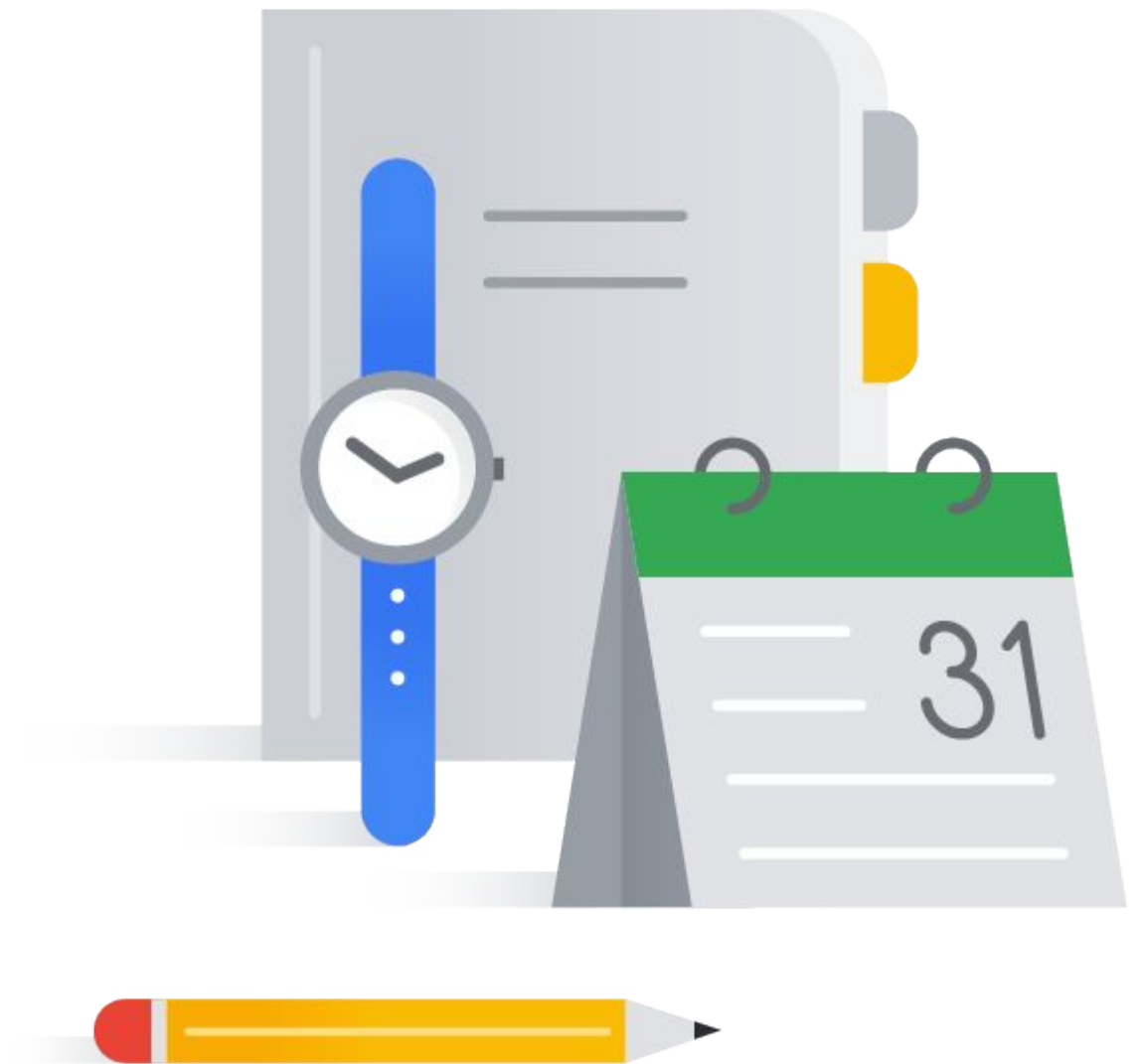


**Who am I and
what's my role here?**



Course agenda

0	Introduction
1	Designing and Planning a Cloud Solution Architecture
2	Managing and Provisioning a Solution Infrastructure
3	Designing for Security and Compliance
4	Analyzing and Optimizing Technical and Business Processes
5	Managing Implementation and Ensuring Solution and Operations Reliability
6	Case Study Preparation and Your Next Steps



Understand the scope of the exam based on the Professional Cloud Architect

[Exam Guide.](#)

In short, the exam tests your skills in:

- Designing **scalable** and **secure** solutions on Google Cloud
- Managing and operating Google Cloud infrastructure
- Understanding and managing **data** in Google Cloud
- Designing and deploying **highly available applications** on Google Cloud
- Managing and **automating** Google Cloud services using APIs and other tools



PCA Exam High-level Overview

- How to position PCA? One of [9 professional level exams](#) (+ [CDL](#) & [Associate Cloud Engineer](#))
- Technically, no hard prerequisites (such as other GCP certs / courses / architect & cloud experience), but...
- **Very broad**, not that deep = Architect, not engineer level (but some implementation details apply)
- 80h-150h+ to complete. Consistency is the key! Learn for 2-3 hours a day, starting from now...
- Exam structure:
 - Multiple-choice questions, asking about “real-world” challenges. Most with a single correct answer, some with more (you will know how many). Get a feeling by doing a [sample test](#).
 - In a lot of cases, you will need to choose OPTIMAL answer from 2-4 which are technically correct (focus would be on time / flexibility / availability / cost / automation / security etc).
 - NO labs, NO hands-on exercises on the exam (but essential when preparing!)
 - 50 questions / 2h for the exam. **Pro tip: Handle the easier questions first (aim at ~1.5 min per question), mark the rest for review. Also, don't leave any questions unanswered (no negative points).**
 - English language only (no additional time for non-native speakers).
 - ~25% (~12 out of 50) of questions based on Case Studies!
- When you submit the exam, you'll only see PASS / FAIL.
 - You will NOT be presented with any details of accuracy / areas to improve etc.
 - It's not clear what is the percentage needed to pass (aim at 85+% accuracy for practise questions).
- Can be taken online or at a testing center. Sign up [here](#).
- Certificate is valid for 2 years (no “delta” exams).
- If you fail, retake policy is: 14 days / 60 days / 1 year (**separate voucher needed for each attempt**)

Exam question - example

Notice the business context

You work for an international company and manage many GCE instances using SSH and RDP protocols.

For security reasons, management asks you that VMs can no longer have external IPs.

How can you fulfil this request, while still being able to manage those VMs?

- ☐ Use Bastion Hosts
- ☐ Use NAT instances
- ☐ Use IAP TCP Forwarding
- ☐ Use Security Command Center

Case studies

- ~25% of the questions (~12/50) on the certification exam will refer to a case study.
- 4 case studies available for analysis **before** the exam (NO NEW CASE CASE STUDIES ON THE EXAM!):
 - [EHR Healthcare](#)
 - [Helicopter Racing League](#)
 - [Mountkirk Games](#)
 - [TerramEarth](#)
- You will have access to a full case study during the exam (but it's not the best time to start analysis...)
- We shall have a **high-level** discussion on those during our meetings (weeks 3-6)

EHR Healthcare

Company overview

EHR Healthcare is a leading provider of electronic health record software to the medical industry. EHR Healthcare provides their software as a service to multi-national medical offices, hospitals, and insurance providers.

Solution concept

Due to rapid changes in the healthcare and insurance industry, EHR Healthcare's business has been growing exponentially year over year. They need to be able to scale their environment, adapt their disaster recovery plan, and roll out new continuous deployment capabilities to update their software at a fast pace. Google Cloud has been chosen to replace their current colocation facilities.

Case study - sample question

For this question, refer to the [Mountkirk Games](#) case study.

Mountkirk Games wants to set up a real-time analytics platform for their new game. The new platform must meet their technical requirements. Which combination of Google technologies will meet all of their requirements?

- ☐ A. Cloud Dataflow, Cloud Storage, Cloud Pub/Sub, and BigQuery
- ☐ B. Cloud SQL, Cloud Storage, Cloud Pub/Sub, and Cloud Dataflow
- ☐ C. Container Engine, Cloud Pub/Sub, and Cloud SQL
- ☐ D. Cloud Pub/Sub, Compute Engine, Cloud Storage, and Cloud Dataproc
- ☐ E. Cloud Dataproc, Cloud Pub/Sub, Cloud SQL, and Cloud Dataflow



Company overview

An online direct-to-consumer Chicago-Based footwear and apparel retailer founded in 2008 and acquired in 2010.

Initiatives and challenges

- Delivery by Drone (BETA)
- Partner APIs
- Social Integration Service (Proof of Concept)

Pro tip: Make notes while you learn!!!

- Choose your favourite tool that handles text **and images**.
- Copy & paste from GCP documentation / course transcripts
- Copy & paste important slides / images / decision trees / tables
- Use colours / bold
- Paste difficult quiz questions from quizzes etc with explanations / links to solutions
- Remember about 2-year validity of GCP certificates -> notes will most probably be very useful next time.
- **Switch between resources if you get bored.**

Custom roles

<https://cloud.google.com/iam/docs/creating-custom-roles>

Use the [gcloud iam list-testable-permissions](#) command to get a list of permissions that are available for custom roles in a specific project or organization. The response lists the permissions that you can use in custom roles for that project or organization.

To list permissions that are available in custom roles for a project or organization, run this command:

```
gcloud iam list-testable-permissions full-resource-name\  
--filter="customRolesSupportLevel!=NOT_SUPPORTED"
```

You can create a custom role at the project or organization level. = NOT ON FOLDER LEVEL!!

To view the role metadata, use one of the methods below:

```
gcloud iam roles describe role-id
```




Example:

```
gcloud iam roles describe roles/iam.roleViewer
```

```
description: Read access to all custom roles in the project.  
etag: AA==  
includedPermissions:  
- iam.roles.get
```

Pro tip no.2: be curious!

[← Create Instance Group](#)

-  **New managed instance group (stateless)**
Automatically manage groups of VMs that do stateless serving and batch processing.
 -  **New managed instance group (stateful)**
Automatically manage groups of VMs that have persistent data or configurations (such as databases or legacy applications).
 -  **New unmanaged instance group**
Manually manage groups of load balancing VMs.

☐ Single zone

☒ Multiple zones

Region * us-central1 (Iowa)

Zones
us-central1-c, us-central1-f, and us-central1-b

Target distribution shape

Even

Distribute managed instances evenly across zones

Balanced

Distribute managed instances as evenly as possible across zones given availability of resources in each zone

Any


Deploy managed instances to one or multiple zones based on availability of resources and reservations in each zone

Use autoscaling to automatically add and remove instances to the group for periods of high and low load. [Learn more](#)

Autoscaling mode

On: add and remove instances to the group

Minimum number of instances * 

Maximum number of instances * 

To maximize availability, the minimum number of instances should be at least equal to the number of zones. Additional instances will be placed in different zones.

Distributing instances using regional managed instance groups

Pro tip no.3: use GCP Free Trial 300USD (*) and Free Tier

It will help you be curious :)

- **90-day, \$300 Free Trial:** New Google Cloud and Google Maps Platform users can take advantage of a 90-day trial period that includes \$300 in free Cloud Billing credits to explore and evaluate Google Cloud and Google Maps Platform products and services. You can use these credits toward one or a combination of products.

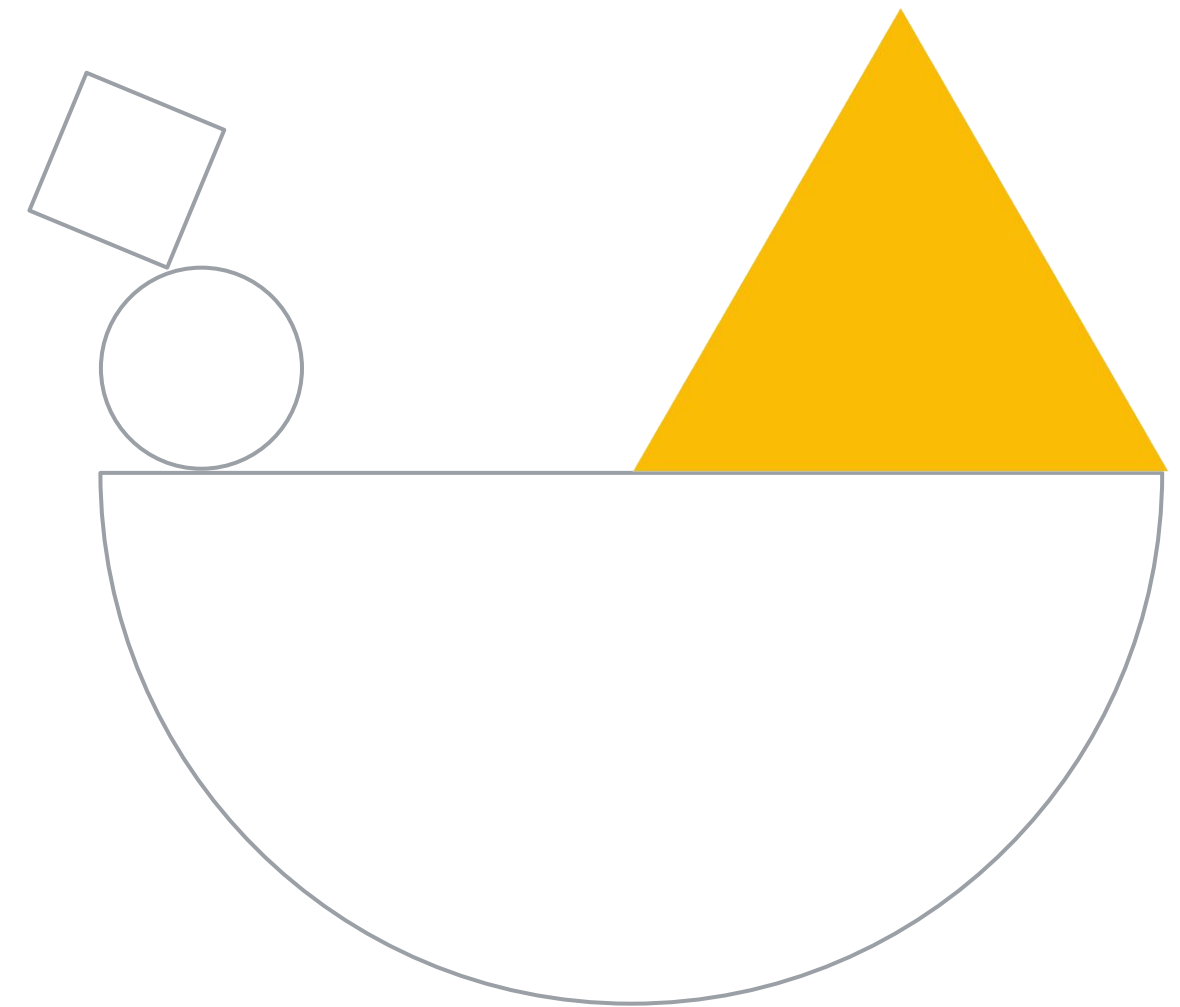
<https://cloud.google.com/free>

Thanks for signing up. Your free trial includes \$300 in credit to spend over the next 90 days. If you run out of credit, don't worry — you won't be billed unless you [turn on automatic billing](#).

GOT IT

* To complete your Free Trial signup, you must provide a [credit card or other payment method](#) to set up a Cloud Billing account and verify your identity. Don't worry, setting up a Cloud Billing account does not enable us to charge you. You are not charged unless you explicitly enable billing by upgrading your Cloud Billing account to a paid account.

Resources to support your certification journey



Diagnostic Questions: example



Your existing application runs on **Ubuntu Linux VMs** in an **on-premises hypervisor**. You want to deploy the application to Google Cloud with **minimal refactoring**.

What should you do?

- A. Set up a **Google Kubernetes Engine (GKE) cluster**, and then create a deployment with an autoscaler.
- B. Isolate the core features that the application provides. Use **Cloud Run** to deploy each feature independently as a microservice.
- C. Use X or Partner Interconnect to **connect the on-premises network where your application is running to your VPC**. Configure an endpoint for a global external HTTP(S) load balancer that connects to the existing VMs.
- D. Write Terraform scripts to deploy the application as **Compute Engine instances**.

Quizzes - planned for weeks 2-6

How to implement back-out/rollback plan for website with 100s of VMs, when the site has frequent critical updates? *

- ☐ Create a Nearline copy of static data in Cloud Storage.
- ☐ Create a snapshot of each VM prior to update, in case of failure.
- ☐ Use managed instance groups with the “update-instances” command when starting a rolling update.
- ☐ Only deploy changes using Deployment Manager templates.



- Aim: validate **technical** knowledge (no business context)
- NOT as complex as questions on the exam

Final exam-like quiz

~30 questions; Link to be shared during our last meeting

One of the developers on your team deployed their application in Google Container Engine with the Dockerfile below. They report that their application deployments are taking too long. You want to optimize this Dockerfile for faster deployment times without adversely affecting the app's functionality. Which two actions should you take? Choose 2 answers.

```
FROM ubuntu:16.04

COPY . /src

RUN apt-get update && apt-get install -y python python-pip

RUN pip install -r requirements.txt
```

- ☐ Remove Python after running pip
- ☐ Remove dependencies from requirements.txt
- ☐ Use a slimmed-down base image like Alpine Linux
- ☐ Use larger machine types for your Google Container Engine node pools
- ☐ Copy the source after the package dependencies (Python and pip) are installed



Exam Tip: aim at 85%+ accuracy before signing up for the exam (don't know what's the passing score, remember?)

Cloud Architecture Center

Cloud Architecture Center

FILTER BY

Choose a topic

[Select all](#)

☐ Security and compliance

FEATURED

☐ Big data and analytics

FEATURED

☐ Artificial intelligence and machine learning (AI/ML)

FEATURED

☐ Application development

☐ Compute

☒ Containers

☐ Databases

☐ DevOps

☐ Financial services

☐ Healthcare and life sciences

Filter results

Containers

X

Refactoring a monolith into microservices

This reference guide is the second in a four-part series about designing, building, and deploying microservices. This series describes the various...

Cloud SQL

Google Kubernetes Engine (GKE)

Cloud Trace

Learn more

Implementing canary deployments with Spinnaker and Istio

Spinnaker is an open source, continuous delivery system led by Netflix and Google. It's used to manage application deployment on various...

Cloud Monitoring

Google Kubernetes Engine (GKE)

Learn more

[Cloud Architecture Center](#)

GCP Services - exam relevance

= “when will I know enough?”

- VERY subjective, NOT a Google-owned or recommended.
- Should be treated as supplemental study materials; NOT an exhaustive list or requirements.
- If it helps -> use it. If it looks scary to you -> don't 😊

		Professional Cloud Architect (PCA)		
0: not covered on the exam at all				0: none
1: basics (high-level functionality and use-cases)				1: basics
2: medium (1 + prerequisites, limitations, common IAM roles, ability to integrate with other services, most common architectures)				2: medium
3: advanced (2 + being able to deploy, troubleshoot and manage)				3: advanced
4: expert (3 + know every detail about the service in complex configurations - huge scale, HA, DR etc)				4: expert
		Recommended minimum knowledge level for PCA	My knowledge level (self-assessment)	
Compute Environment				
	Compute Engine (GCE)	3: advanced	0: none	
	Managing access to VMs (OS Login etc)	2: medium	0: none	
	Persistent Disks	3: advanced	0: none	
	GCE Instance Groups	2: medium	0: none	
	Multi-NIC VMs	1: basics	0: none	
	App Engine flexible environment	2: medium	0: none	
	App Engine standard environment	2: medium	0: none	
	Cloud GPUs	1: basics	0: none	
	Migrate for Compute Engine	1: basics	0: none	
	VMware Engine	1: basics	0: none	
	Cloud Run	2: medium	0: none	
	Cloud Functions	2: medium	0: none	
	Bare Metal Solution	1: basics	0: none	
	GCVE	1: basics	0: none	
	Preemptible VMs	2: medium	0: none	
	Sole-tenant Nodes	2: medium	0: none	
	Local SSD	1: basics	0: none	
	VM Manager	1: basics	0: none	
PCA ▾ PCSE ▾				

[LINK](#) (go to “PCA” tab)

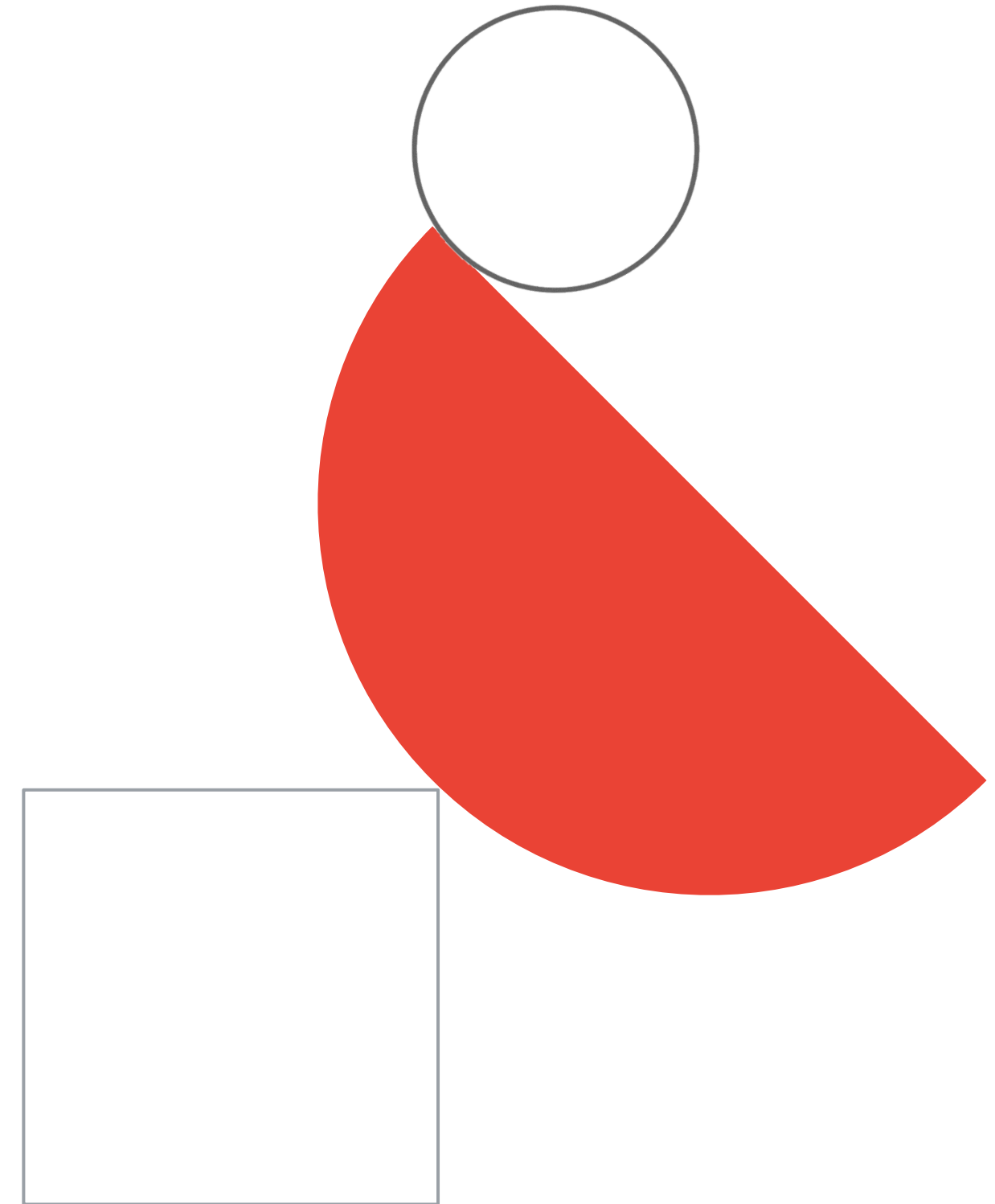
See what others think...

Published	Title/Link	Author
2022/10	How I passed the GCP PCA Exam	Geoffrey
2022/07	The Architect and the Helicopter Racing	Aliaksei Kaliutau
2022/06	GCP PCA RoadMap & Resources	Shubham Chaurasia
2021/08	Path to Google Cloud Professional Cloud Architect Certification	Vinny Joseph
2021/06	GCP Professional Cloud Architect — Exam Guide Mapping to Prep links	Ramesh Rajini
2021/03	My Review of the PCA BETA Exam	Antoni Tzavelas
2021/01	How I prepared for GCP PCA exam?	Rakesh Vardan
2020/09	How to pass PCA – as a sales guy	Rolf Siegel
2020/03	Build on Your Experience to Earn Cloud Certifications	Joshua Fox
2020/02	PCA Prep Sheet	Ammett Williams
2019/07	How to pass the Cloud Architect and Data Engineer GCP certifications	Ivam Luz
2019/03	Professional Cloud Architect Certification	Mete Atamel
2019/01	Notes from my GCP PCA Exam	Sathish VJ
2019/01	5 Tips to Become a GCP PCA	Janakiram MSV

[LINK](#)

Cloud Skills Boost Demo

Tips and comments to the course content

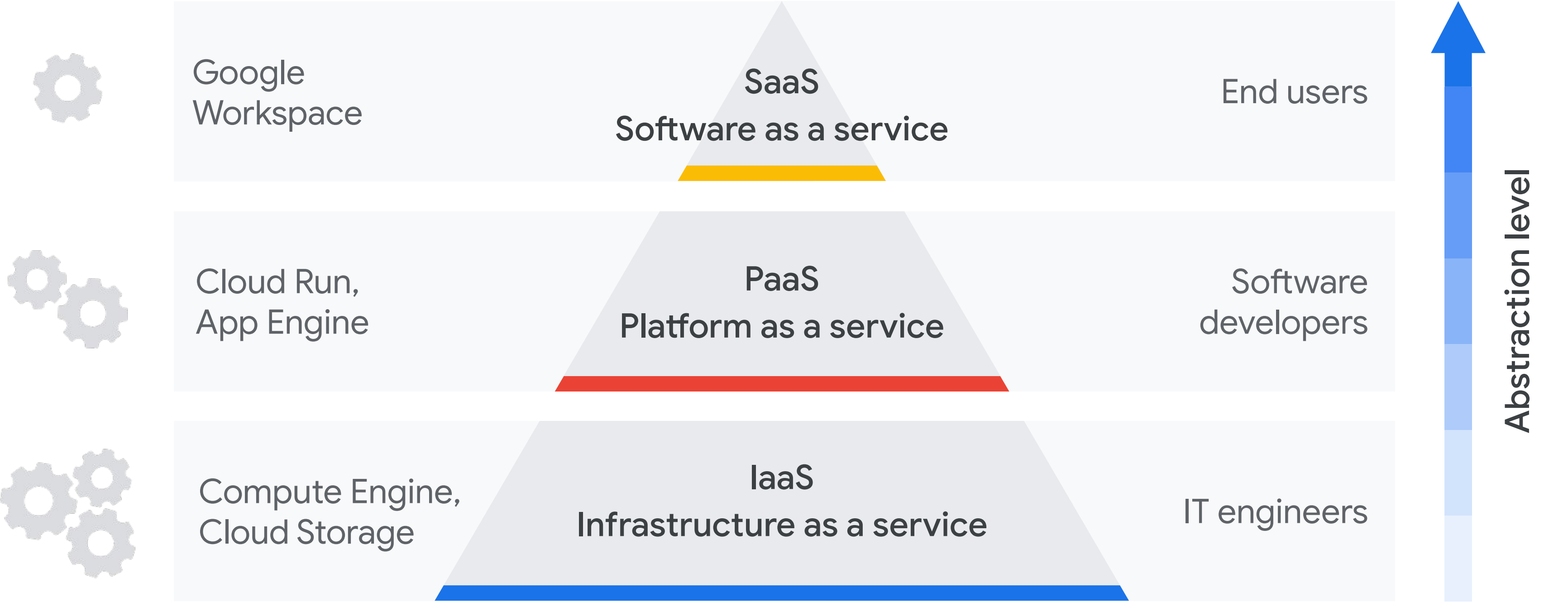


Opex vs Capex

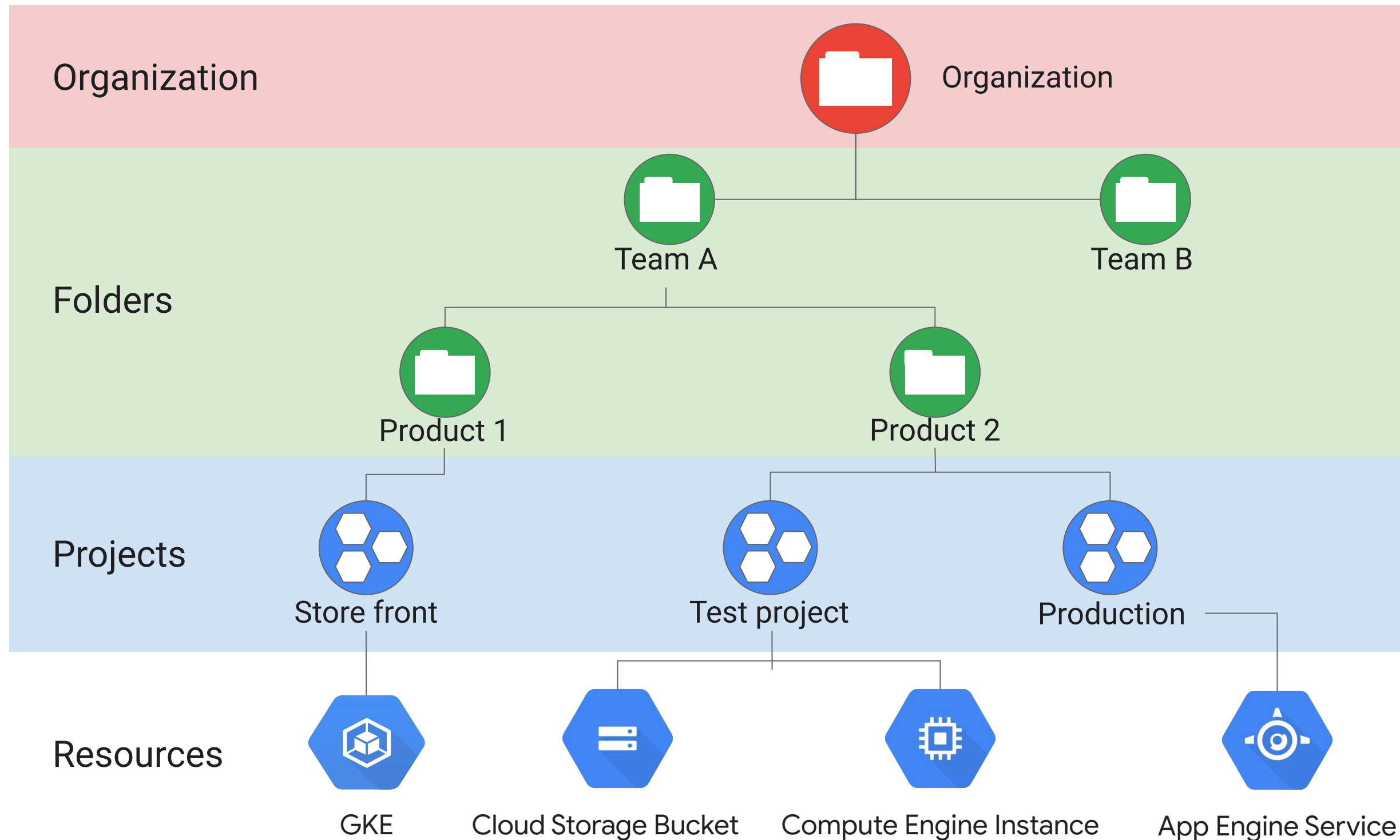
- [CAPEX Vs OPEX - Fundamentals of Cloud #shorts - YouTube](#)
- **Capex:**
 - Traditional, “on-premises” approach. Eg. build a datacenter, but hardware and licenses, amortize over time (years)
 - An organization purchases computing capacity upfront and uses it over time.
 - Easy, but usually not flexible.
- **Opex:**
 - Cloud-native approach. Eg. spin up a storage service and use it as needed (decommission after few days; resize when needed; stop outside of business hours)
 - Based on pay-as-you-go approach, with no upfront payments. Resources and services are available on-demand, often billed based on per-second usage fees.
 - Harder to predict costs (and spend fluctuates each month), but you gain a ton of flexibility (has effects on sizing, time to deliver etc).

Exam Tip: Despite Opex is the cloud-native approach, there are ways to cost-optimize workloads by committing to long-term (1-3 years) usage, this leaning towards Capex model a bit.

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 Organization 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

AUTHORIZATION



Cloud Identity



Cloud IAM

2SV WITH GOOGLE AUTHENTICATION

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



SMS / Voice



Backup codes



Authenticator (TOTP)



Google prompt (Mobile Push)



Security Key

Phishable SS7 vuln
SIM Swap

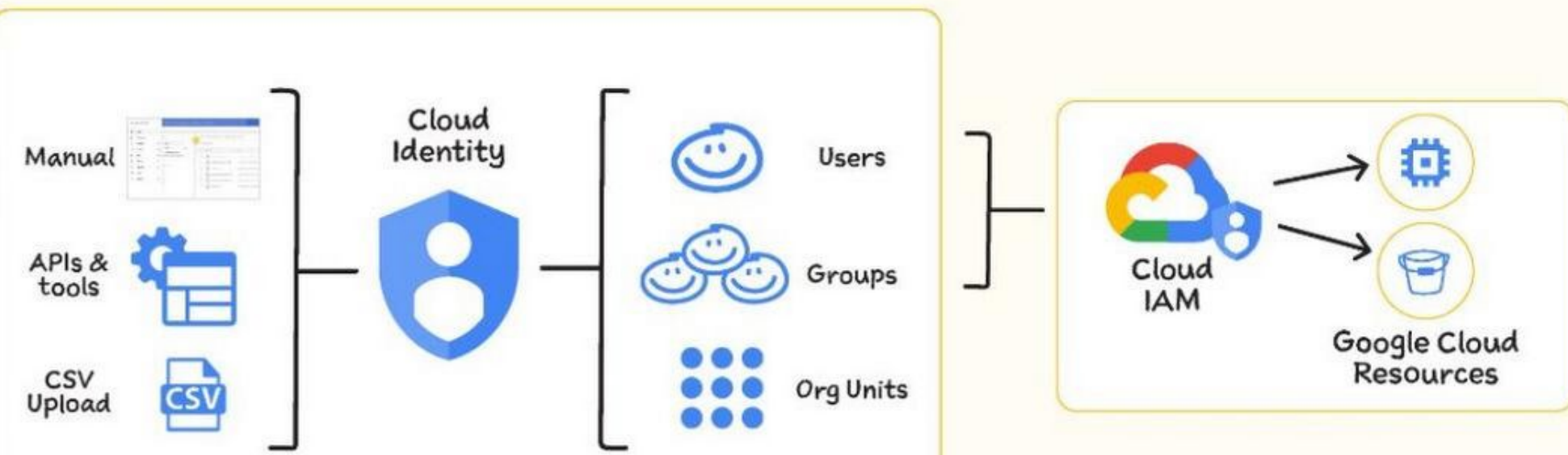
Phishable

Phishing-resistant

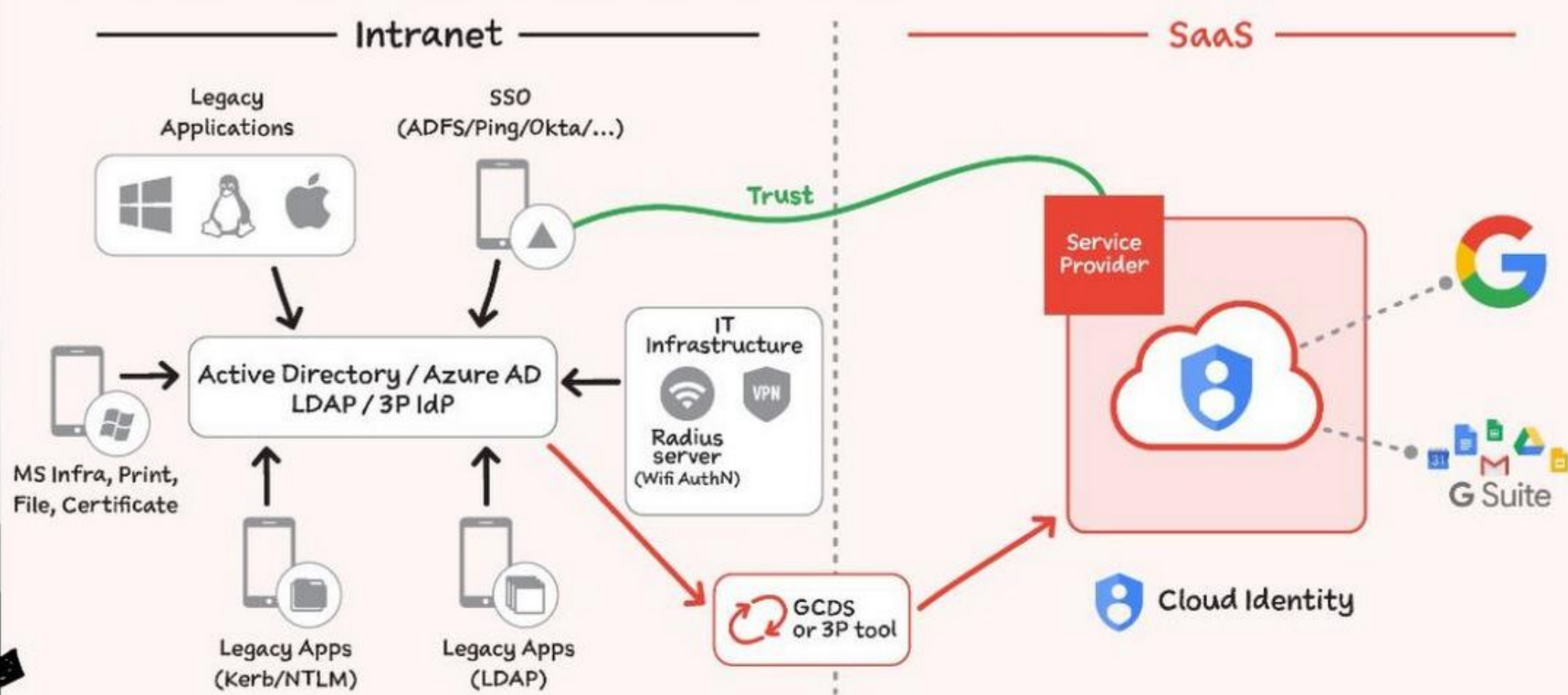
BEST PRACTICE

INCREASED ASSURANCE

WHAT IS CLOUD IDENTITY (AUTHENTICATION)?



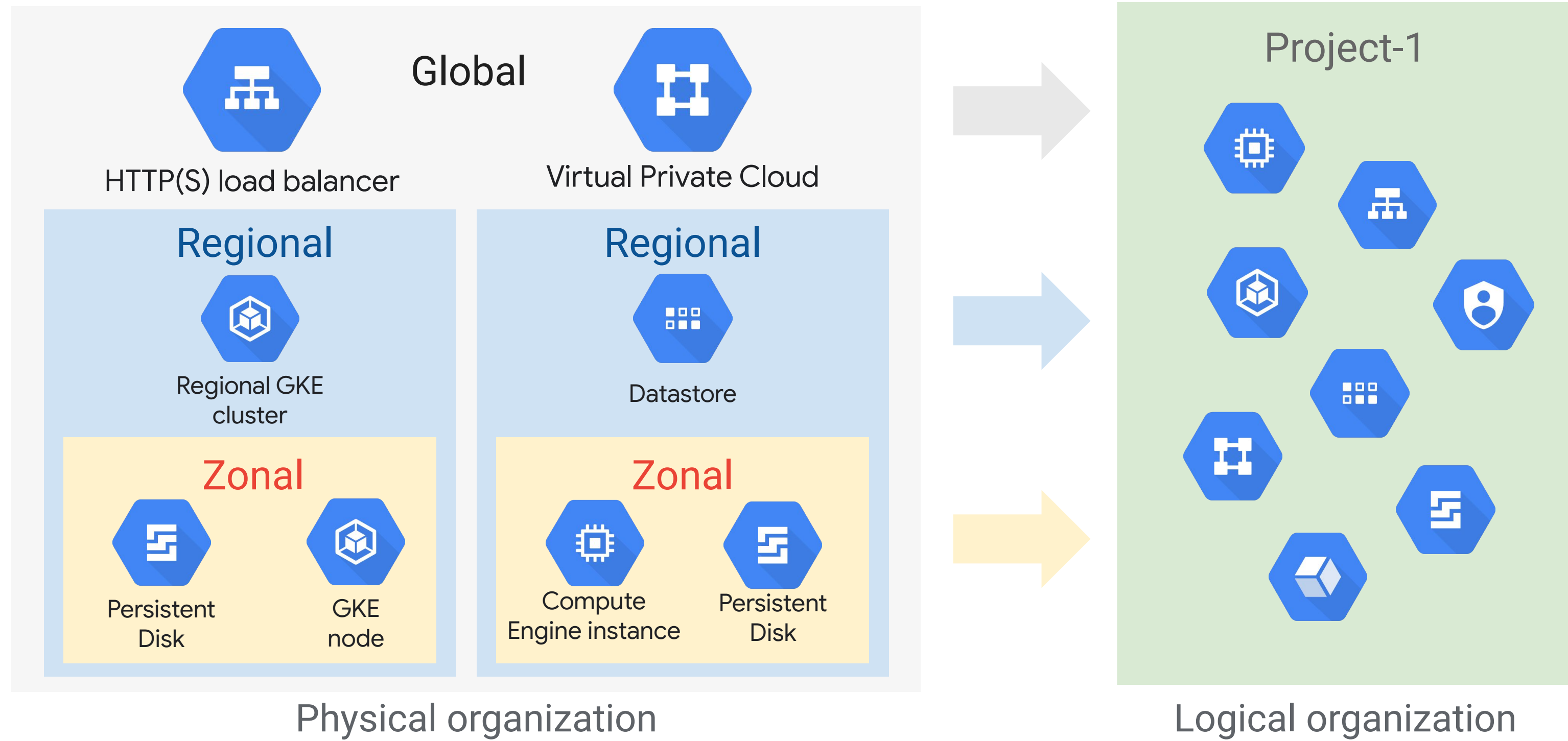
THIRD-PARTY AS AN IDENTITY PROVIDER: TYPICAL ARCHITECTURE



Organization Policy vs IAM Policy

Organization Policies	IAM Policies
Constraints that allow you to: <ul style="list-style-type: none">• 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

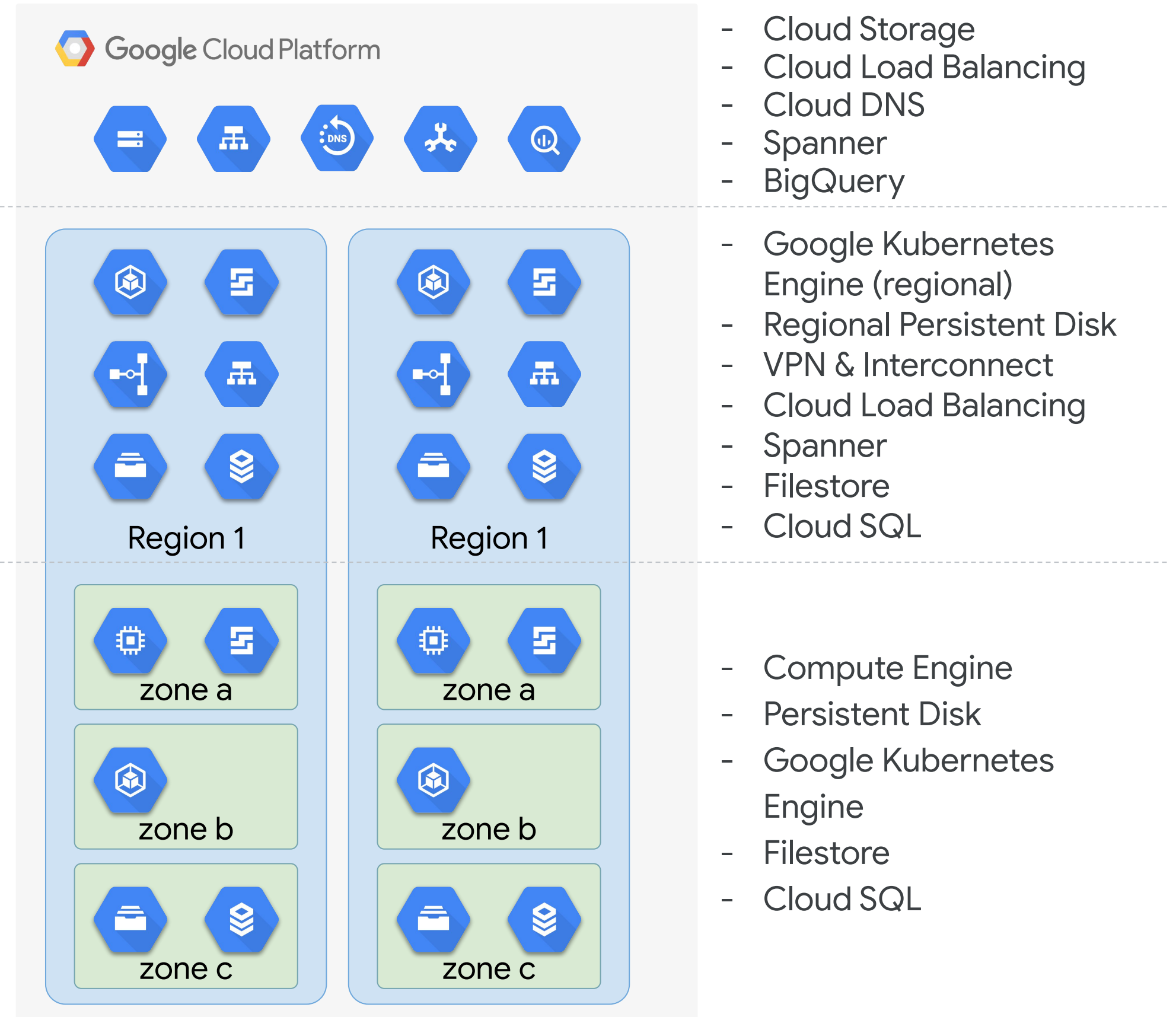


- Not all services provide regional availability, and not all regional services are made equal. Regional deploy may have RTO & RPO > 0 (e.g.: minutes for regional Cloud SQL).
- DNS updates may take longer than expected (TTL, caching).
- Restoring a VM from a snapshot gives you a new VM with a different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

Multi-regional

Regional

Zonal



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!

