Google Developer Experts

Designing a Scalable and Secure Cloud Architecture for the Future

Ananda Dwi Ae
@misskecupbung

Experts 2023

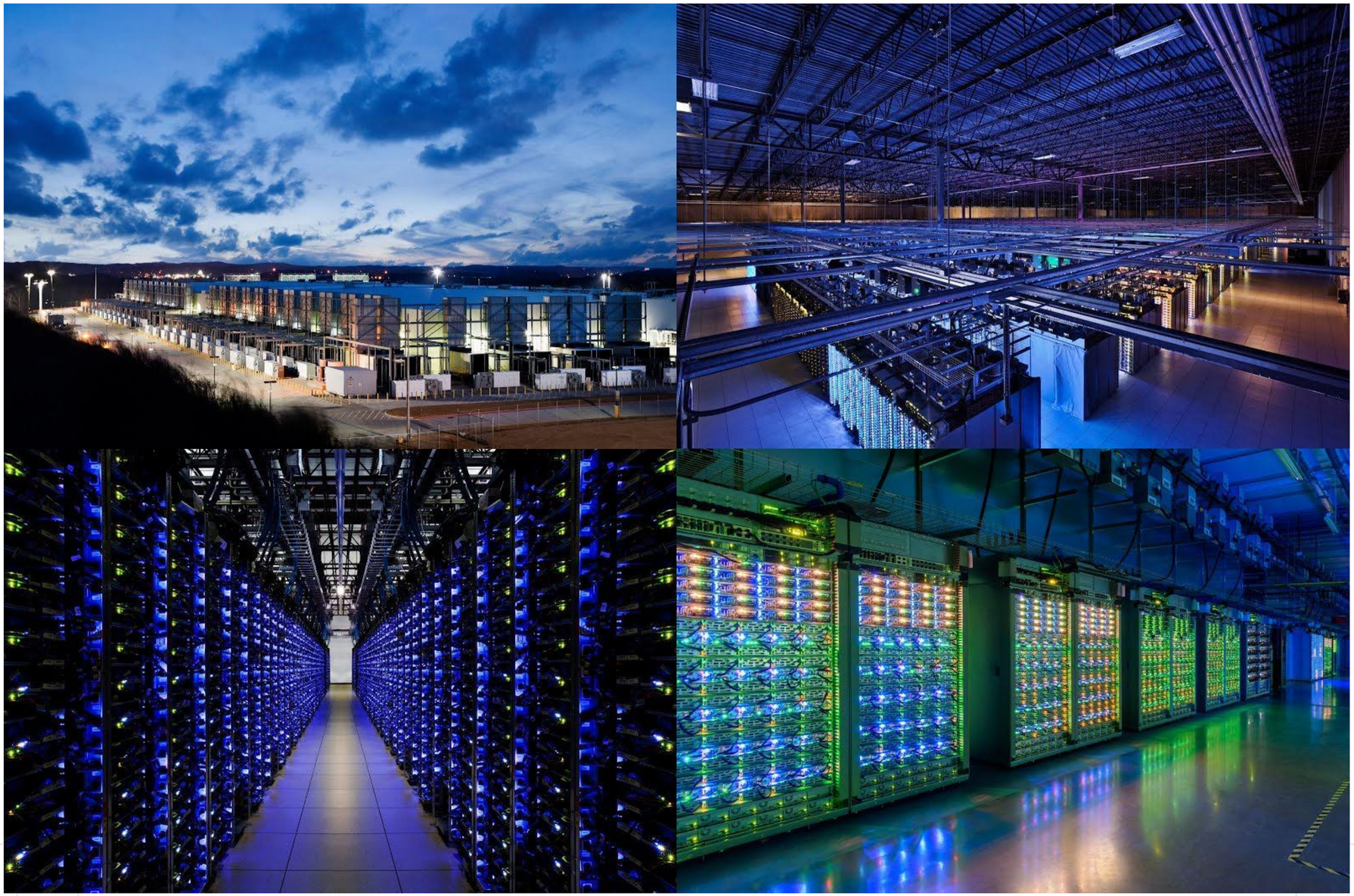
Google Cloud Platform

Google Cloud Platform

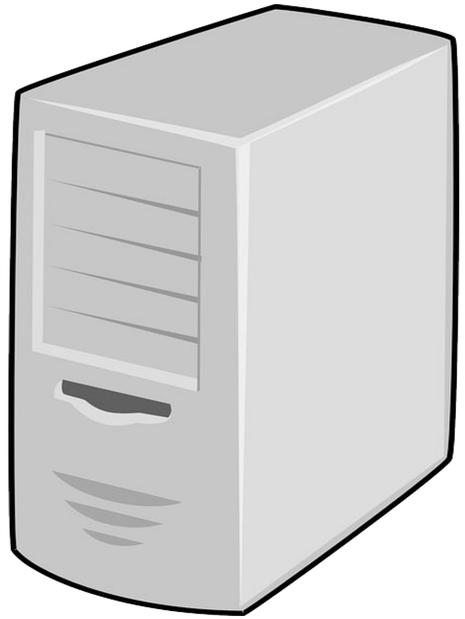
Hello World!

Ananda Dwi Rahmawati

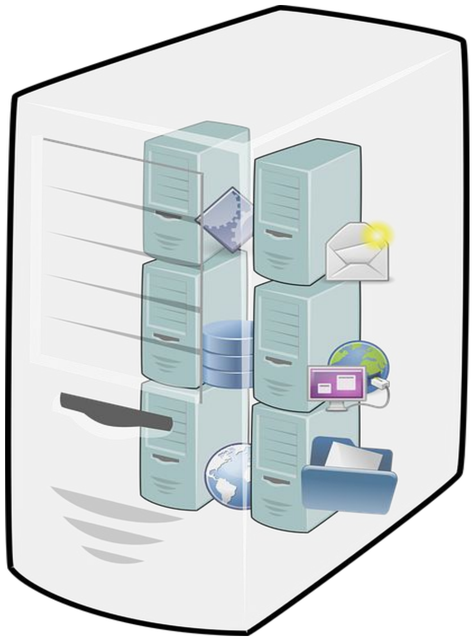
- Cloud Engineer @ Activate Interactive Pte Ltd Singapore | 2023 - present
- 4+ years experience
- Google Developer Expert Cloud - Modernization Architecture
- Tech background: System, Networking, IaaS & PaaS Cloud, DevOps, a bit of Programming
- https://linktr.ee/misskecupbung



A virtual machine is a software-based computer



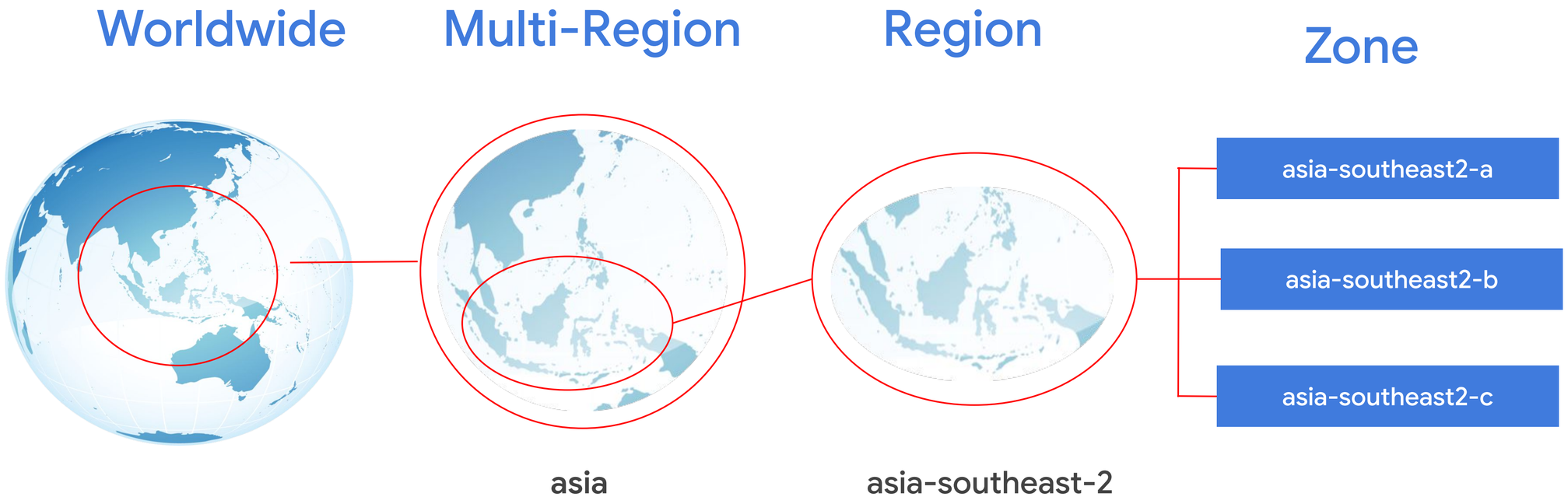
Physical Computer

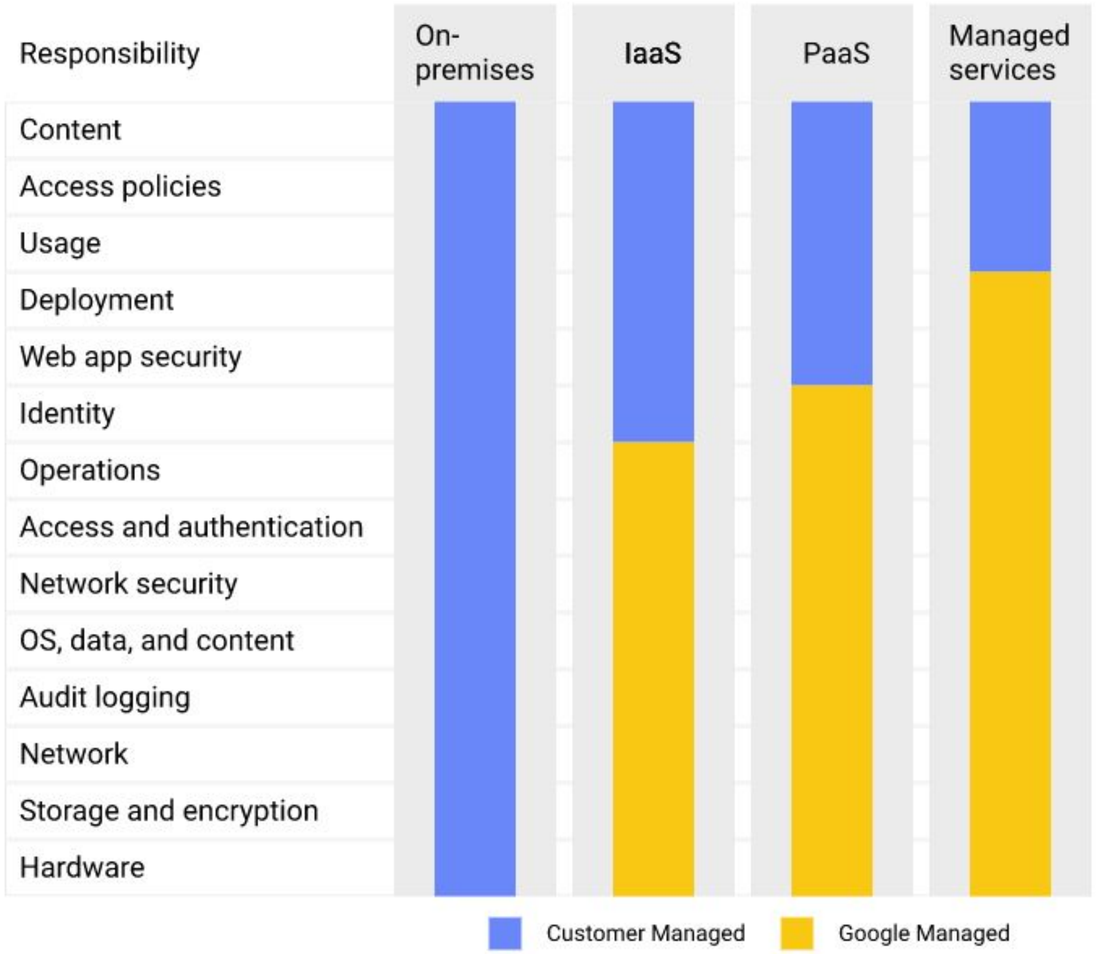


Virtual Machines in a Physical Computer


Oregon
Salt Lake City
Las Vegas
Los Angeles
Toronto
Montréal
Iowa*
Columbus
N Virginia
S Carolina
Dallas
Mexico
Netherlands
Finland
London
Berlin
Belgium
Warsaw
Frankfurt
Paris
Zurich
Turin
Milan
Madrid
Tel Aviv
Dammam
Delhi
Doha
Mumbai
Seoul
Tokyo
Osaka
Taiwan
Hong Kong
Singapore
Jakarta
São Paulo
Santiago
Johannesburg
Sydney
Melbourne
Current region with 3 zones
Future region with 3 zones

Jakarta region




Responsibility
On-premises
IaaS
PaaS
Managed services
Content
Access policies
Usage
Deployment
Web app security
Identity
Operations
Access and authentication
Network security
OS, data, and content
Audit logging
Network
Storage and encryption
Hardware
Customer Managed
Google Managed

Cloud Services

Infrastructure

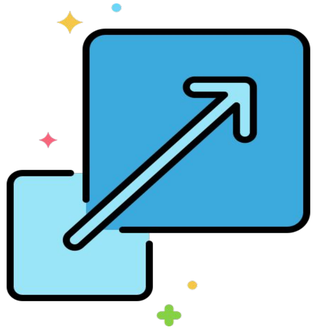
Platform

Software

... as a service

Benefits of Cloud Computing

Cost savings



Scalability

Security

Reliability

No need to managed your own infrastructure. Use managed service instead

Application Data

Cloud Storage

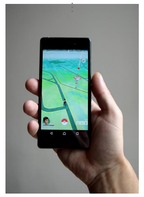
Cloud Datastore

Cloud Bigtable

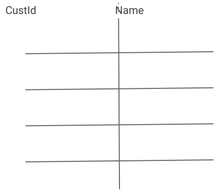
Cloud SQL

Cloud Spanner

Object data like multimedia



High-volume or semi-structured data like streaming or gaming data



Relational data

Application Logic

App Engine

Container Engine

User data management

API gateways
for other backend apps

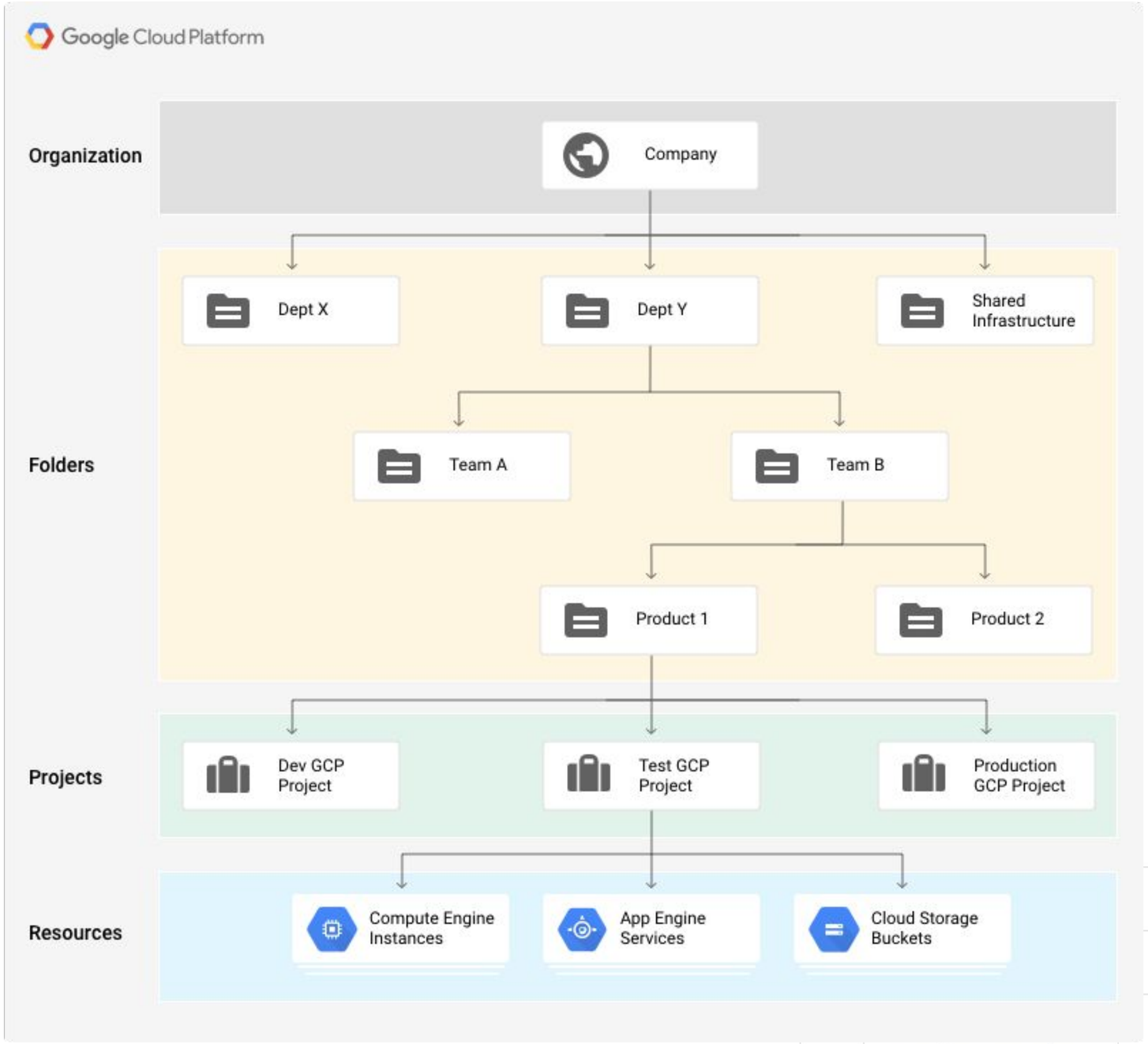
Payment etc.

Integration with other Google services

Google Maps, YouTube, and more

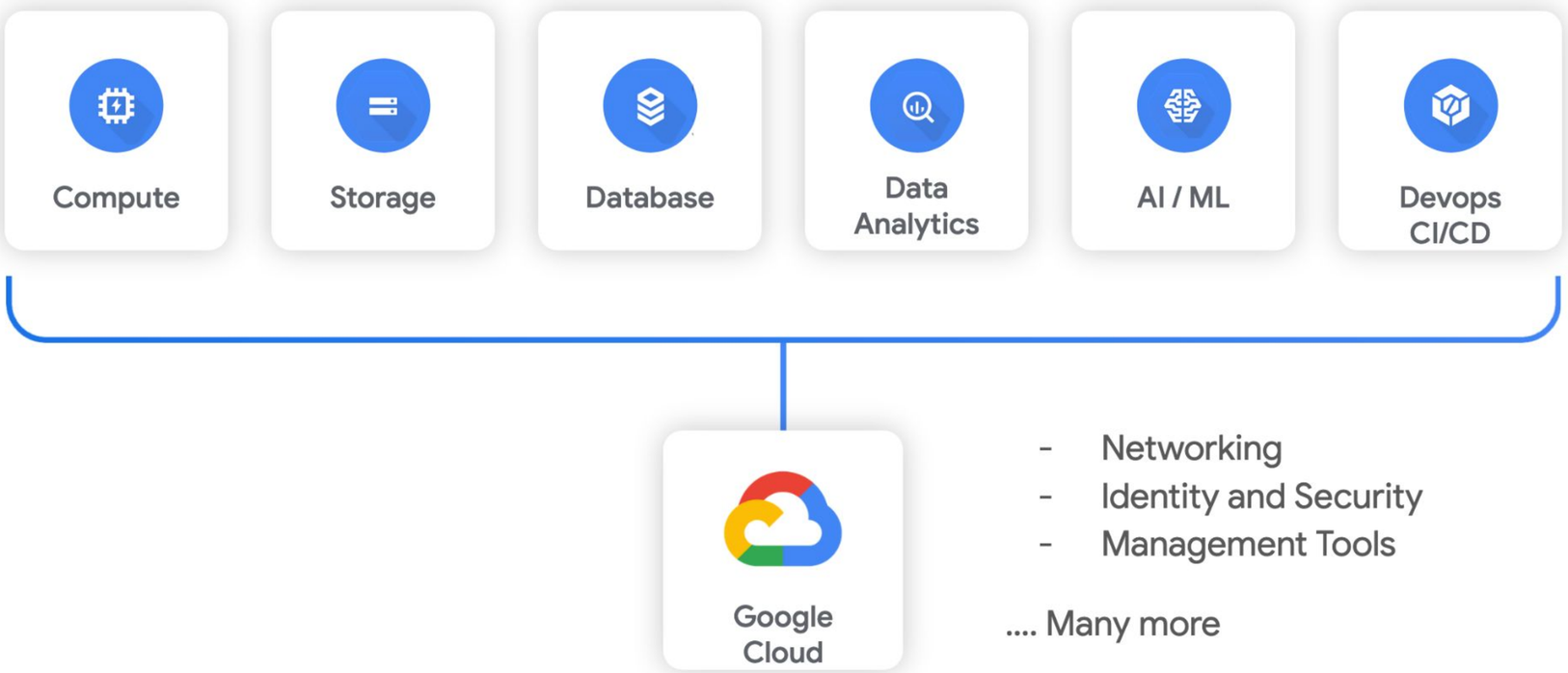
GCP Resources Hierarchy

- **Projects** : Base hierarchy level. Every resource is associated with a project.
- **Folders** : Provide additional grouping mechanism between projects. They can be nested.
- **Organization** : Represent an organization and the root node of Google Cloud resource hierarchy



Experts

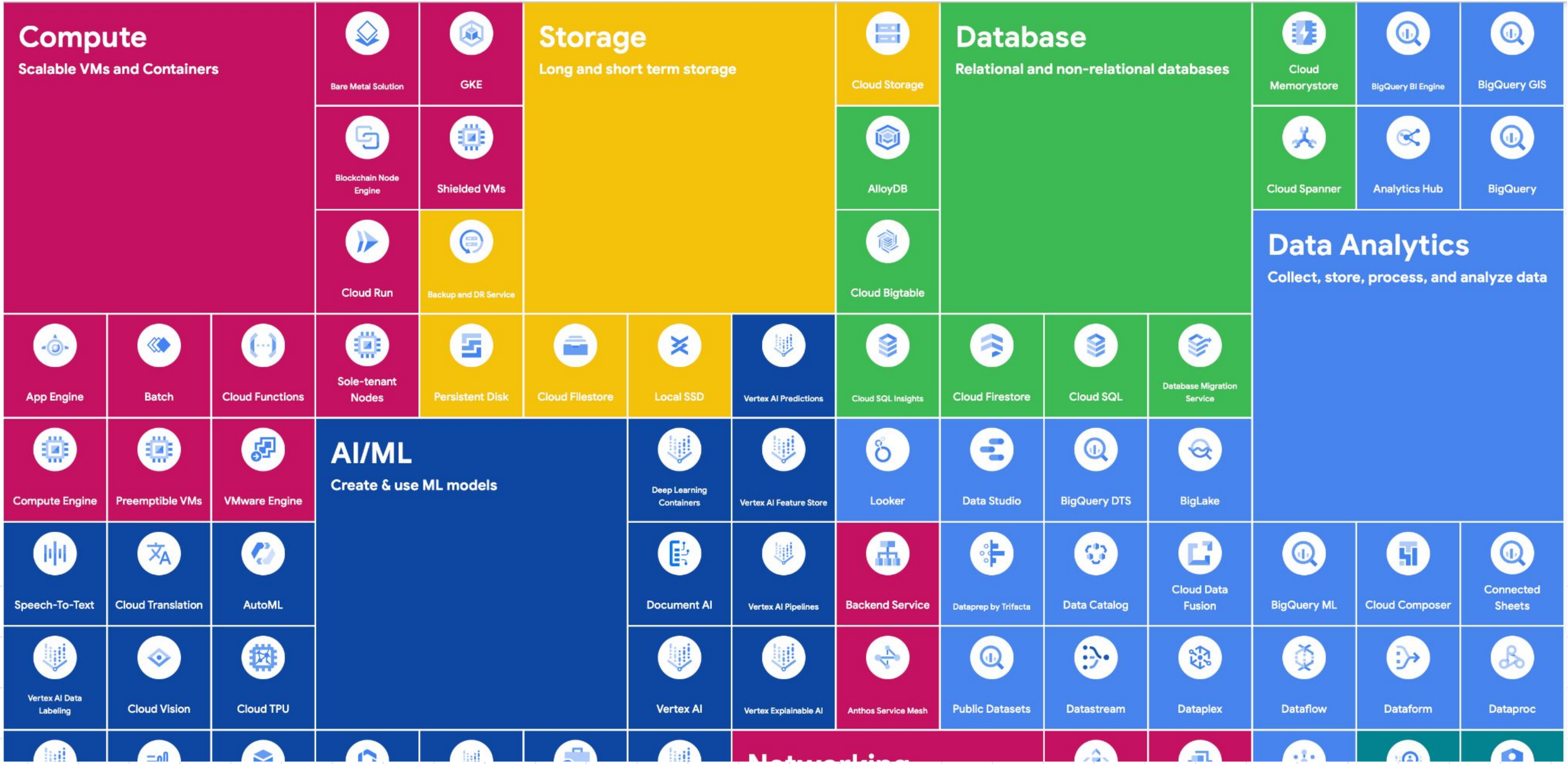
Google Cloud Platform (GCP)



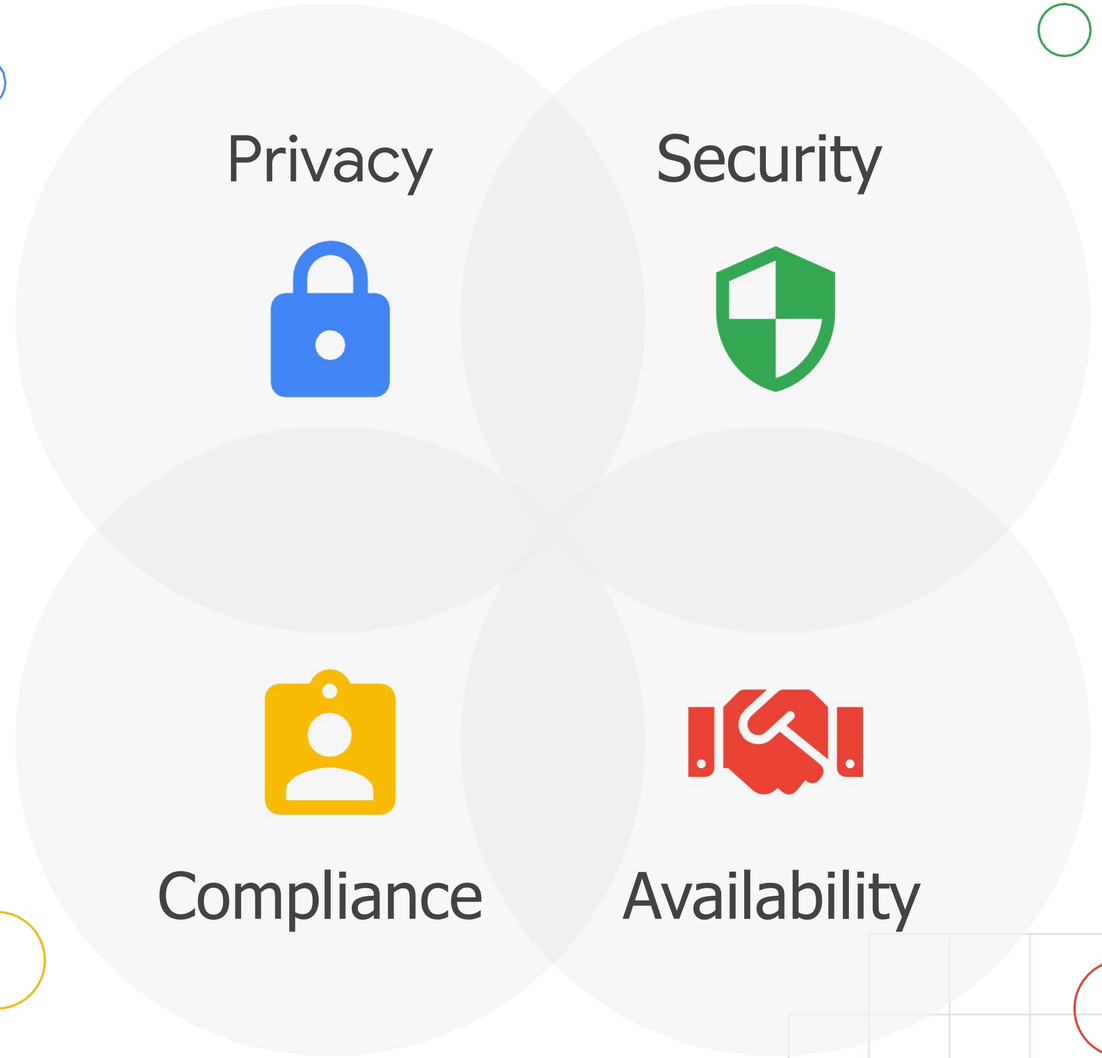
Google Cloud

Get started

Developer cheat sheet | Map view | List view | Get the poster on GitHub | Architecture



Fundamental terms:



Google Cloud Security fundamentals

Protection

Secure core infrastructure designed, built, and operated to help prevent threats

Control

Security controls to help meet policy, regulatory, and business objectives

Compliance

Working to meet our responsibilities and make compliance easier for customers

Compliance Offerings

Global

ISO/IEC 27001
ISO/IEC 27017
ISO/IEC 27018
SOC 1
SOC 2
SOC 3
PCI DSS
CSA STAR
MPAA
Independent Security Evaluators Audit

Americas

USA

HIPAA
HiTrust
FedRAMP
FIPS 140-2
COPPA
FERPA
NIST 800-53
NIST 800-171
NIST 800-34
Sarbanes- Oxley
SEC Rule 17a-4(f)
CFTC Rule 1.31(c)-(d)
FINRA Rule 4511(c)
HECVAT
DISA IL2
CCPA

Canada

Personal Information & Electronic Documents Act
Personal Health Information Protection Act

Argentina

Personal Data Protection Law

Europe, Middle East & Africa

Europe

GDPR
EU Model Contract Clauses
Privacy Shield
TISAX
EBA Guidelines

Germany

BSI C5

Switzerland

FINMA

France

HDS

Spain

Esquema Nacional de Seguridad

South Africa

POPI

UK

NCSC Cloud Security Principles
NHS IG Toolkit

Asia Pacific

Australia

Australian Privacy Principles
Australian Prudential Regulatory Authority Standards
IRAP

Indonesia

PP No. 71 2019

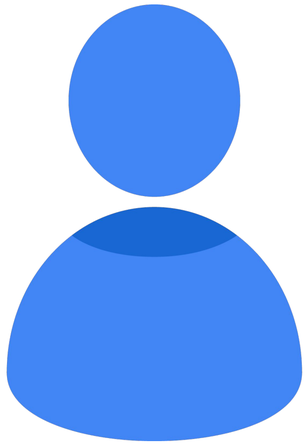
Japan

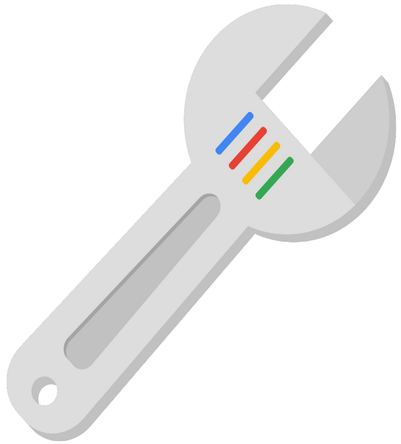
FISC
My Number Act
NISC
CSV Guidelines
3G3M

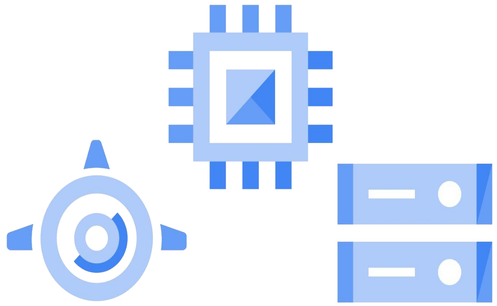
Singapore

MTCS Tier 3
OSPAR
MAS Guidelines
ABS Guide

Identity and Access Management



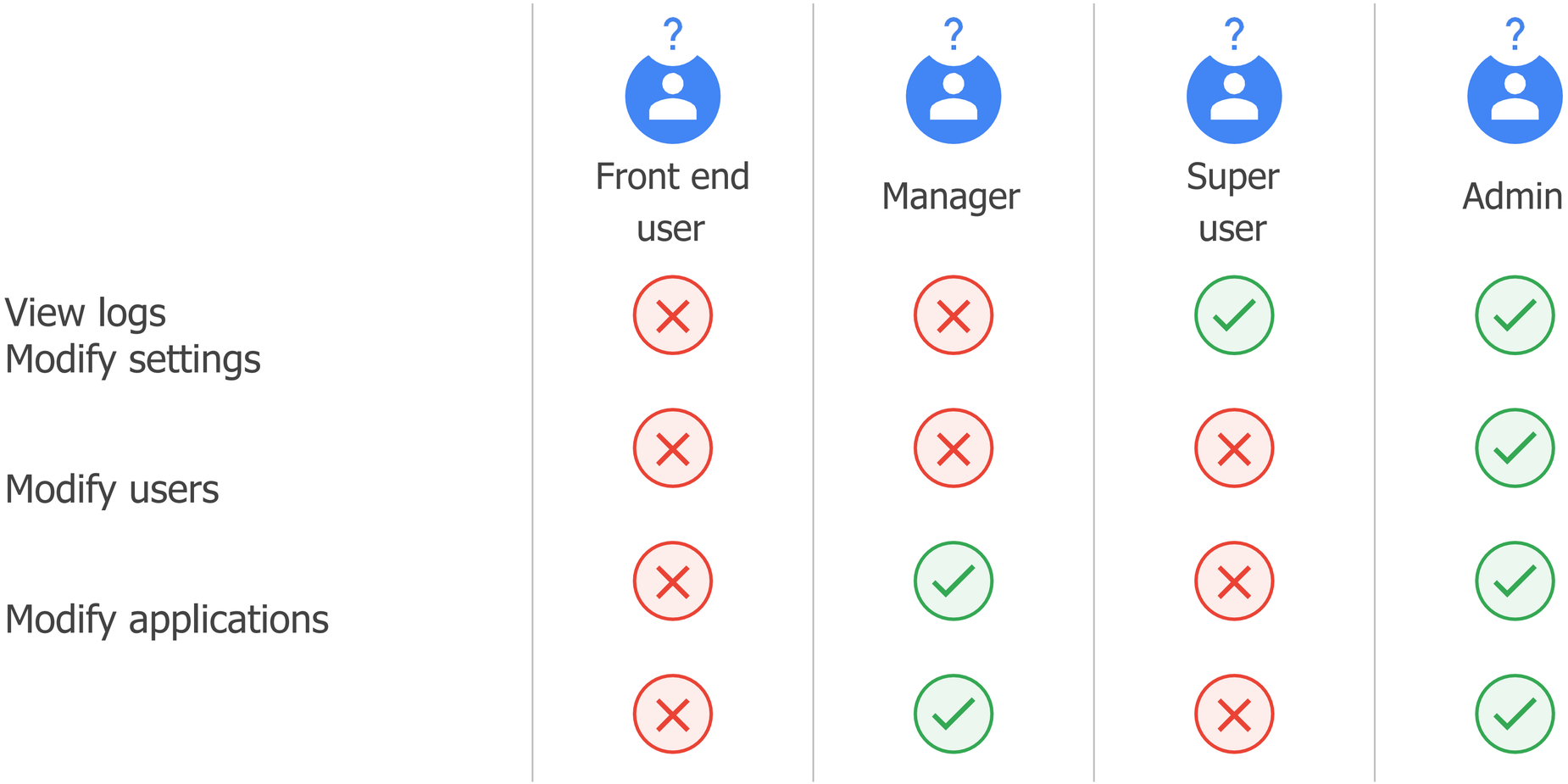




Who

can do what

on which resource



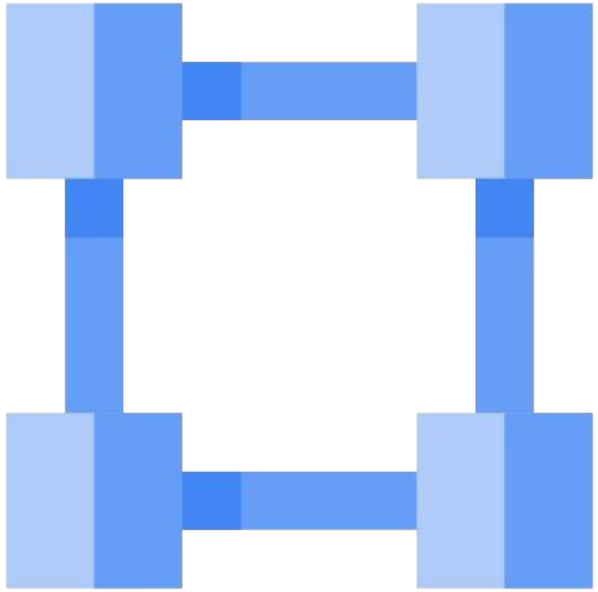
IT teams need to have a complete understanding of who can access what data. Wherever possible, they need to establish granular access policies.

They need to define who can do what, and on what cloud resource.

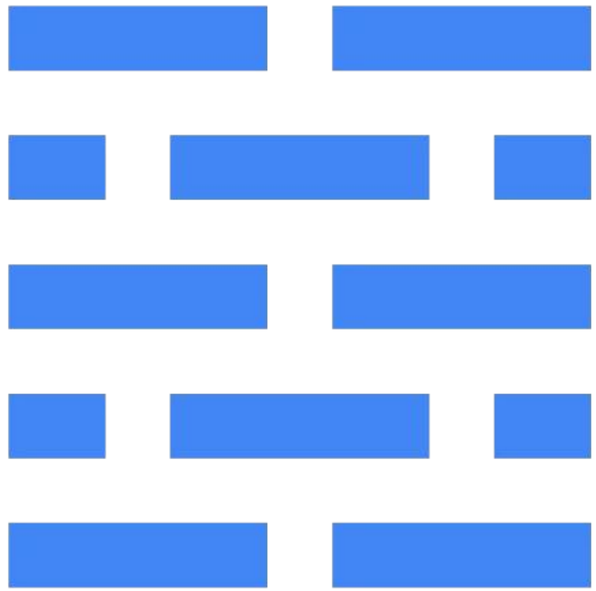
IAM Best Practices

- Adhere to the Principle of Least Privilege
- Use groups when configuring Google Cloud access.
- Assign roles to the groups instead of individual users.
- Utilizing predefined roles offers less administrative overhead
- Predefined roles are managed by Google.
- Custom roles are not maintained by Google.
- Audit logs record project-level permission changes. Audit policy changes.
- Export audit logs to Cloud Storage to store your logs for long periods of time.
- Export audit logs to Cloud Storage to store your logs for long periods of time.

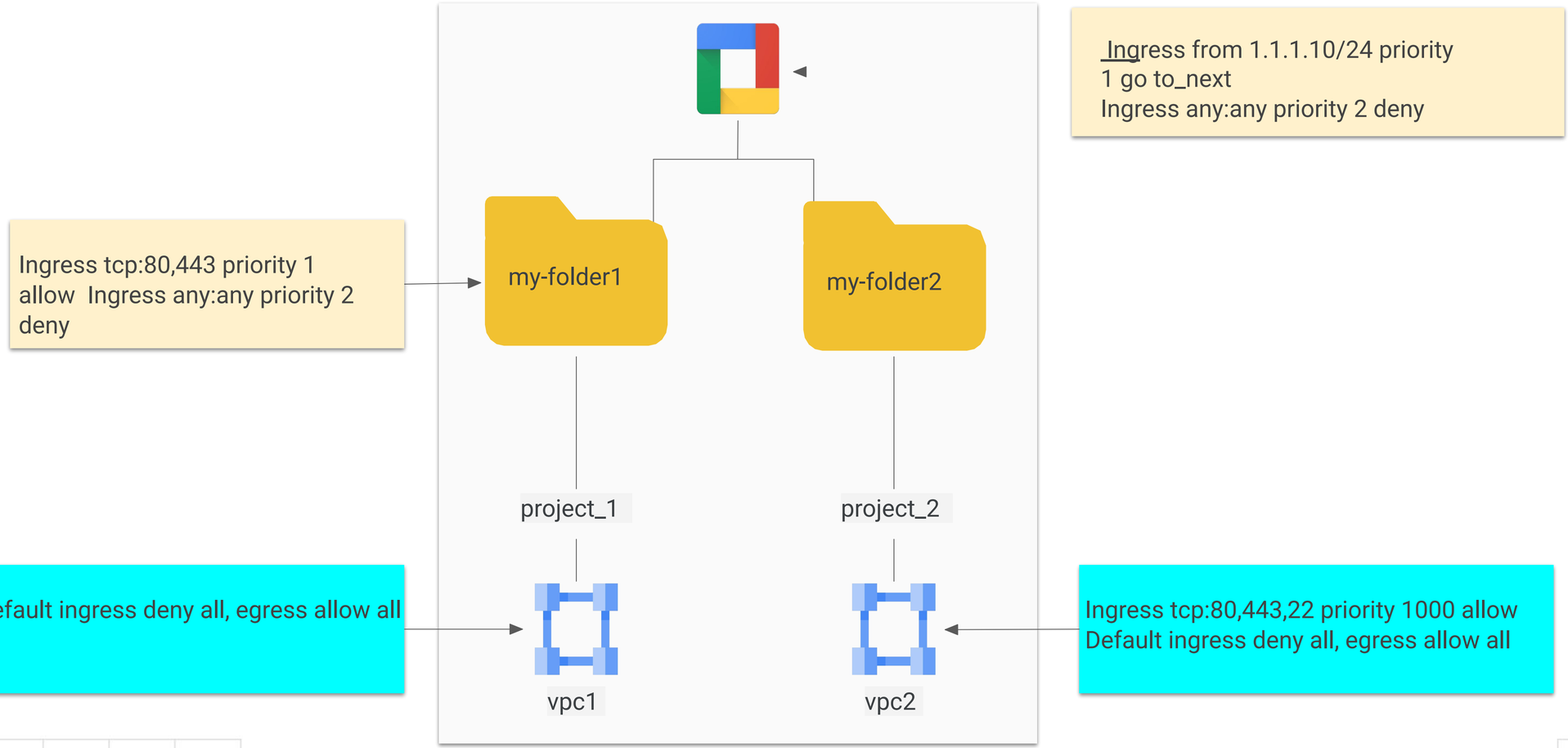
VPC



Firewall rules protect VM instances from unapproved connections



Hierarchical firewall policies



Firewall Best Practices

- Use the model of least privilege.
- Minimize direct exposure to/from the internet.
- Prevent ports and protocols from being exposed unnecessarily.
- Develop a standard naming convention for firewall rules. For example:
  - **{direction}-{allow/deny}-{service}-{to-from-location}**
  - **Ingress-allow-ssh-from-onprem**
  - **egress-allow-all-to-gcevms**
- Consider service account firewall rules instead of tag-based rules.

Experts

Thank You!

Ananda Dwi Ae
@misskecupbung