

Cloud Computing Cloud Security

CIS437

Erik Fredericks // frederer@gvsu.edu

Adapted from Google Cloud Computing Foundations, Overview of Cloud Computing (Wufka & Canonico)

Outline

Types of security

Service accounts / IAM

Securing a handful of services

First off (per usual)

What are some security concerns we have?

And how about privacy?

https://www.youtube.com/watch?v=UixcB9QD_rc

IT security concerns (from the book)

Confidentiality

Integrity

Availability

IT security concerns (from the book)

Confidentiality

- Only those who have the authorization to access data/services ... should
 - Different from authentication ... how?

Integrity

- Data not corrupted or changed by unauthorized users

Availability

- Data accessible
- Working properly for users
- ...what if we lock it away on an airgapped drive?

Threats/Risks

Where do threats come from?

Internal or external?



Who?

- Humans, bots, tech problems, *the environment*

Why?

- Malicious
- Non-malicious
- sell info to highest bidder
- ignorance



Threats/Risks

(Book has a categorized list of various types)

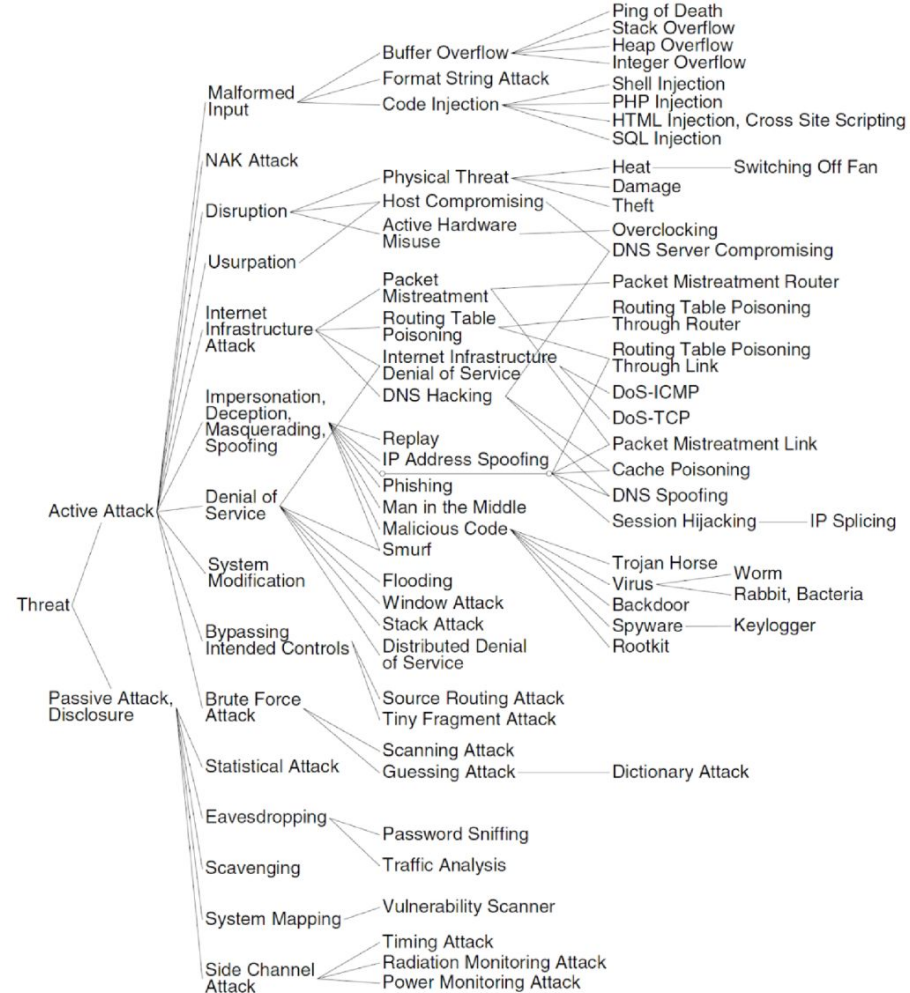


Figure 6.1: Classification of IT Security Threats

Detecting Intrusions (this slide is probably from 2015)

- UNIX security model (without SELinux) has a bit of a flaw...



Detecting Intrusions

- Reliance on superuser security model
 - Processes running with superuser privileges
- If you can coopt a SUID process....

Example

- Flaw in /etc/fingerd
 - Finger service over network
 - Displays information about users
- Possibility of buffer overrun
 - Read in text from standard input
 - No check on length of data read (512 bytes expected...more provided)
 - Overflowed buffer – caused fingerd to execute a shell
 - Shell has root privileges...

Example

- Issue was with C `gets` command
 - All distributions patched their programs to use `fgets`, which allows for size check
- However...
 - `sprintf()` and `strcpy()` commands became popular
 - New vulnerability found years later
 - `sprint()` and `strcpy()` can be called without boundary checking...
 - Patch again!

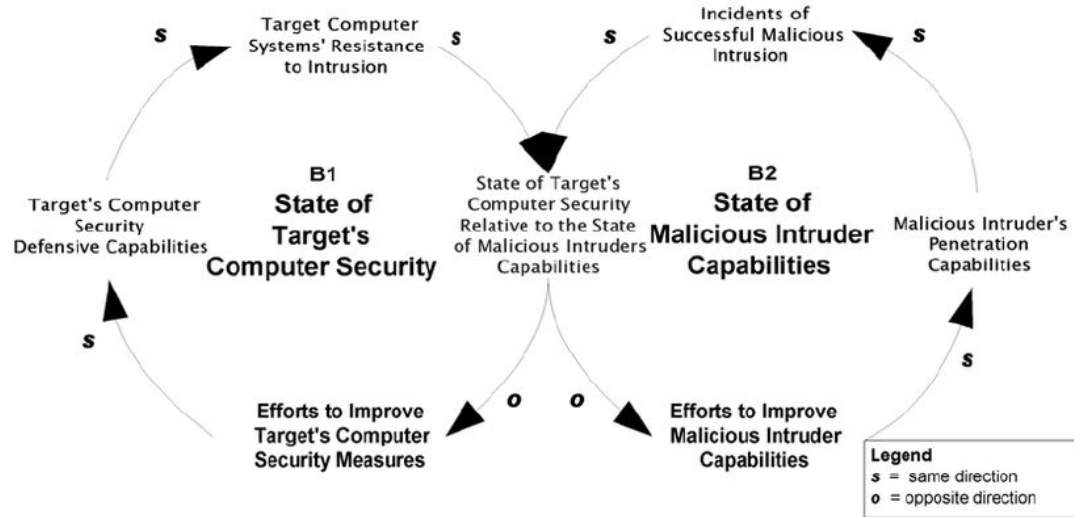
And, if you're managing a VM

KEEP IT UP TO DATE

- https://www.youtube.com/watch?v=8ol_laNhGjE

With managing threats...

It is always an arms race that you must **constantly** stay up on



Back to the cloud specific things...



First, a slightly longer video than normal

But a fascinating report on the issues **you** will be facing
(honestly, in the cloud or not)

<https://www.youtube.com/watch?v=VK0GyUSDwQY>

Types of security

Here, we have **two perspectives** for security

Perimeter security

- Handled by cloud provider
- Firewalls, blocking external access, etc.

Internal security

- Handled by **you**
- Configuring services, setting permissions, etc.

Cloud security models

For your reading (we'll be talking about Google):

Microsoft: <https://docs.microsoft.com/en-us/azure/security/fundamentals/overview>

AWS: <https://aws.amazon.com/compliance/shared-responsibility-model/>

Google Cloud is:

Not responsible for your security concerns

- That's their model
- And honestly, it is pretty reasonable

Consider this to be a sysadmin-style responsibility

- You are running a server, you must:
 - Setup/configure user accounts and access
 - Open/block ports
 - Allow/disallow IP ranges
 - ...
 - Others?
- No real difference here - it is still **your** application you must maintain!

An example from the past (posted to CIS655 page)

Personal example! I had a group of students learning on temporary Windows virtual machines and had them set a password of Temp12345 for a login.

Oddly enough, some of the machines were hacked and turned into a Bitcoin-mining botnet.

Google quickly realized what was happening and shut down the machines and sent me and the students a nasty-gram, however it was a sobering learning experience. How were the machines discovered, you might ask?

Well, there tend to be a lot of bots on the internet constantly scanning for weakpoints, poor passwords, etc. They most likely were targeting Google-specific IP address ranges and were testing for points of failure. Well, they found one!

What does that mean?

Your cloud provider can only do so much

- If you set a weak password, then it will be pretty quickly exploited
- Cloud providers often operate on known IP ranges
 - Or discoverable ports
 - Or known APIs
- Pretty easy to setup a script to automatically ping them for a response!

Meaning, if your provider sets up a giant concrete wall but you use a mesh screen for the door, others will gain access

Your responsibility

Continuously **stay informed** of the latest security threats

Continuously **monitor** your application:

- Who has been accessing it?
- From where?

Properly setup accounts with appropriate access

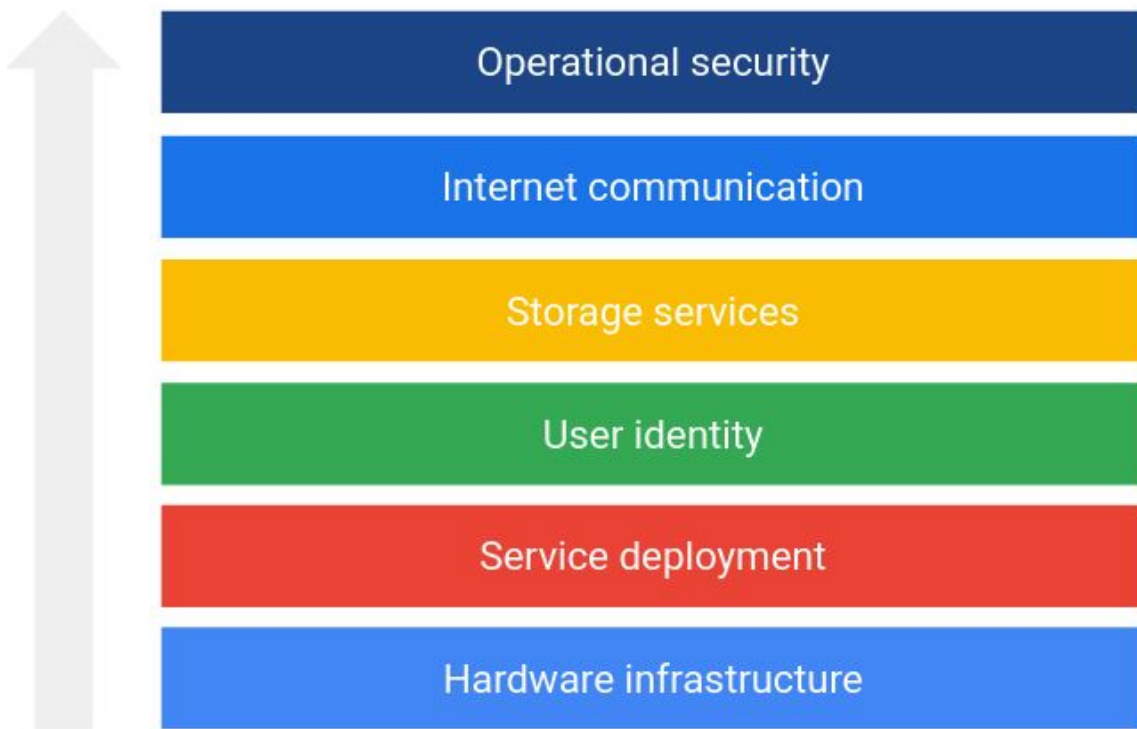
- Principle of least privilege **absolutely applies** here

For example...

<https://cloud.google.com/logging/docs/alerting/log-based-alerts>

- 1) Break a CF
- 2) Go to logging explorer and watch for errors to keep an eye on it and alert when found (shakes fist at those pesky devs)
- 3) ...?
- 4) Profit!

Google's infrastructure security layers



Security layers

Built into every layer of a system, not just the exterior!

- Including hardware!

Why do this?

- Consider the number of users both creating applications and using them
- We are now working at a global scale, not just a handful of users!
- Must minimize as many attack surfaces as possible

Bug bounties

Are you a white hat hacker, perhaps somebody interested in pentesting?

- Bug bounty programs are sometimes a thing!

AWS: <https://aws.amazon.com/security/vulnerability-reporting/>

GCP: <https://bughunters.google.com/>

Azure: <https://www.microsoft.com/en-us/msrc/bounty-microsoft-azure>

Considerations:

- ENSURE YOU ARE DOING LEGAL THINGS (and that there is an actual desire)
 - Don't end up in legal trouble because you think you're being helpful...

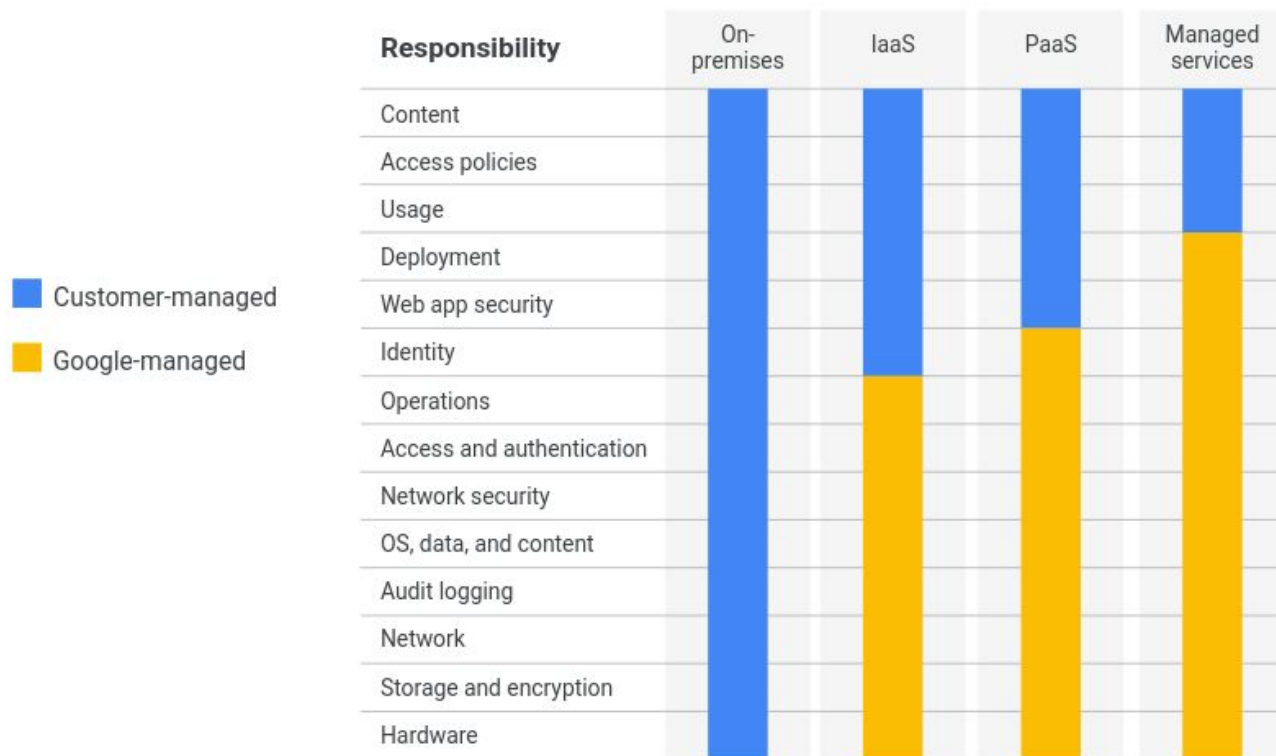
Enough pontificating

Shared security model

- or, what is your responsibility and what is your provider's
- can vary from provider to provider
 - and change over time - stay up to date!

How do you think this works?

With Google Cloud, security responsibility is shared



Responsibility scales

The more your provider ... provides, the more responsibility they have

- and the less access you have to secure it

For example, a virtual machine (IaaS) allows you to create users, set permissions, open/close access, etc.

- You have a lot of control!

However, using a SaaS app (Google Docs, perhaps) really only allows you to configure who has access to it

- Much less control!
 - But you still control who can access it!

CUSTOMER

RESPONSIBILITY FOR
SECURITY 'IN' THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA
ENCRYPTION & DATA INTEGRITY
AUTHENTICATION

SERVER-SIDE ENCRYPTION
(FILE SYSTEM AND/OR DATA)

NETWORKING TRAFFIC
PROTECTION (ENCRYPTION,
INTEGRITY, IDENTITY)

SOFTWARE

COMPUTE

STORAGE

DATABASE

NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS

AVAILABILITY ZONES

EDGE LOCATIONS

AWS

RESPONSIBILITY FOR
SECURITY 'OF' THE CLOUD

Service accounts

Those of you with sysadmin experience (hopefully all of you)

What is a service account when handling Linux/Windows servers?

- Or just a normal machine - that's fine too

Same concept applies here!

- 1) You have a thing that needs managing
- 2) You create an account **specific to that thing**
 - a) Think - program accounts in Linux
- 3) They only have access to **that thing**
- 4) Whenever your app needs to access **that thing** it uses that service account

Service accounts

For example:

- 1) You create a serverless function that calculates the 8-th digit of Pi
 - a) Want $n=8$, receive 6 (3.14159626)
- 2) You don't want this function accessible to the entire world as it can be computationally-expensive
- 3) You create a service account that is the only entity in the world that has access to the Pi-function.
- 4) When you call that function, you login as (or gain access as) that specific account

Service accounts

Can have very broad or very specific access

- Your cloud account has very broad access

Rights can be assigned/re-assigned at will or as needed

Service accounts for project "cloud-apps-demos-w24"

A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. [Learn more about service accounts.](#)

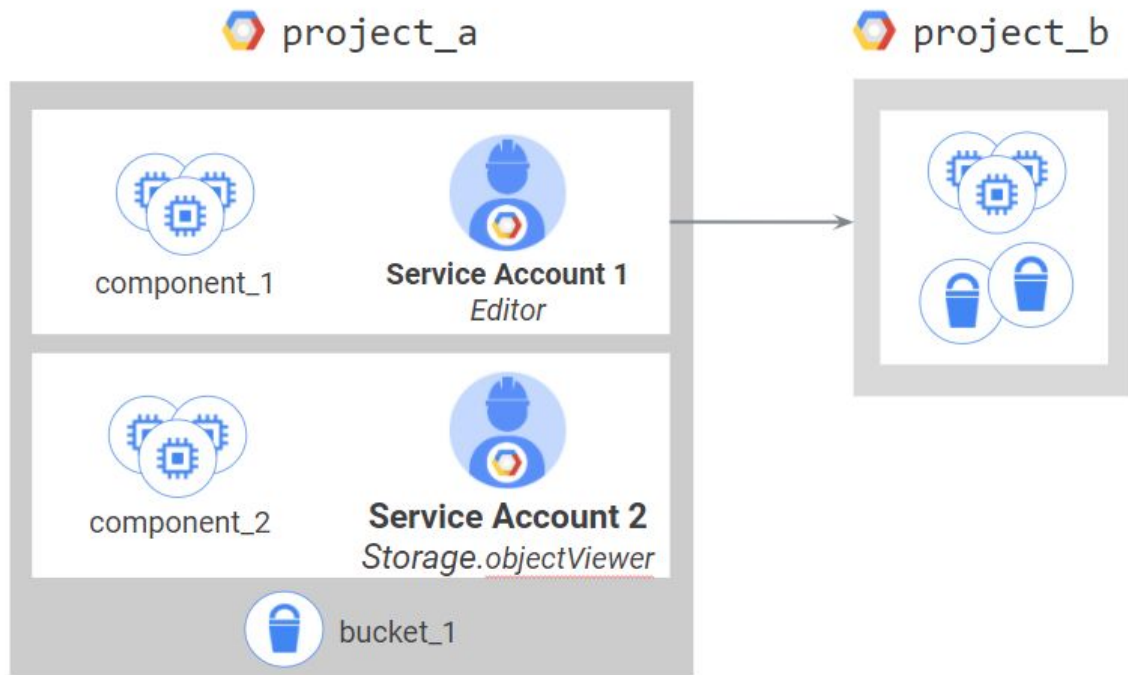
Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload, or the creation of service accounts entirely. [Learn more about service account organization policies.](#)

Filter Enter property name or value								
☐	Email	Status	Name ↑	Description	Key ID	Key creation date	OAuth 2 Client ID ?	Actions
☐	 cloud-apps-demos-w24@appspot.gserviceaccount.com	✔ Enabled	App Engine default service account		No keys		108105512910582852774	⋮
☐	 630329882835-compute@developer.gserviceaccount.com	✔ Enabled	Compute Engine default service account		No keys		102682547958783731337	⋮

Service accounts and IAM

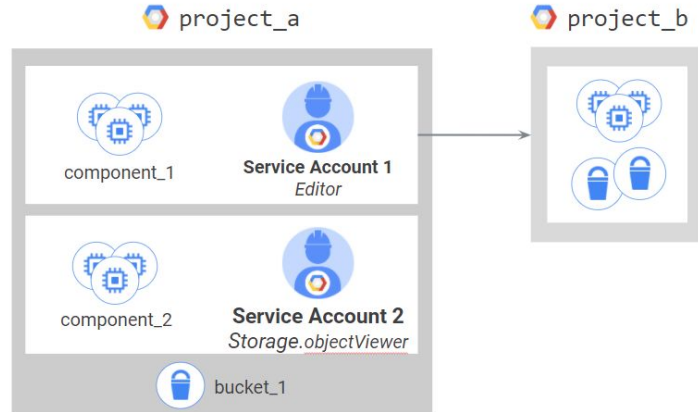


You can grant different groups of VMs in a project different identities

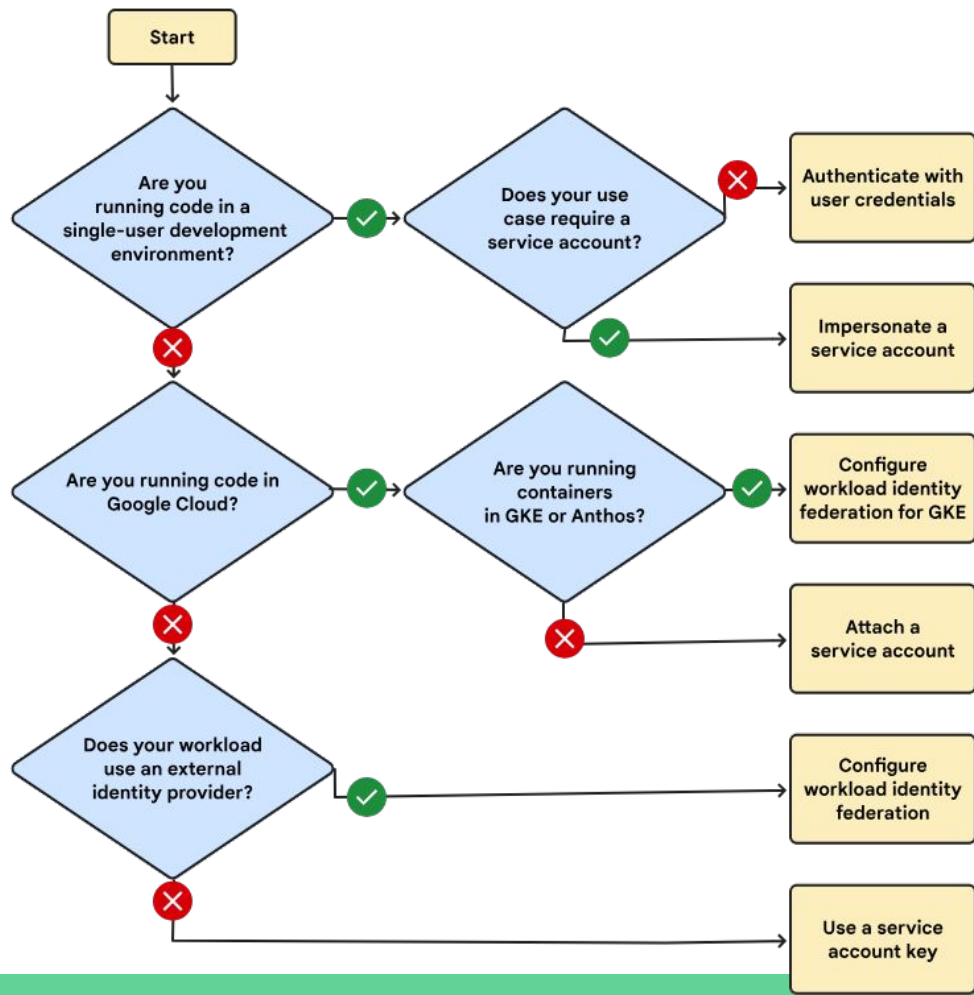


Here's a more complex scenario. Say you have an application that's implemented across a group of virtual machines:

- One component of your application requires the editor role on another project, `project_b`
- But, another component doesn't need any permissions on `project_b`.
- You would create two different service accounts, one for each subgroup of virtual machines.
- In this example, VMs running `component_1` are granted Editor access to `project_b` using Service Account 1.
- VMs running `component_2` are granted `objectViewer` access to `bucket_1` using Service Account 2.
- Service account permissions can be changed without recreating VMs.



<https://cloud.google.com/iam/docs/best-practices-service-accounts>



Identify and Access Management (IAM)

Google Cloud service for handling security (and assigning roles/accounts)

IAM

LEARN

PERMISSIONS

RECOMMENDATIONS HISTORY

Permissions for project "cloud-apps-demos-w24"

These permissions affect this project and all of its resources. [Learn more](#)

2 service accounts with highly privileged roles Owner / Editor have excess permissions.
Improve security by applying recommendations to these accounts.
[Learn more about recommendations.](#)

Tell me more

VUE RECOMMENDATIONS IN TABLE

VUE BY PRINCIPALS

VUE BY ROLES

GRANT ACCESS

REMOVE ACCESS

Filter Enter property name or value

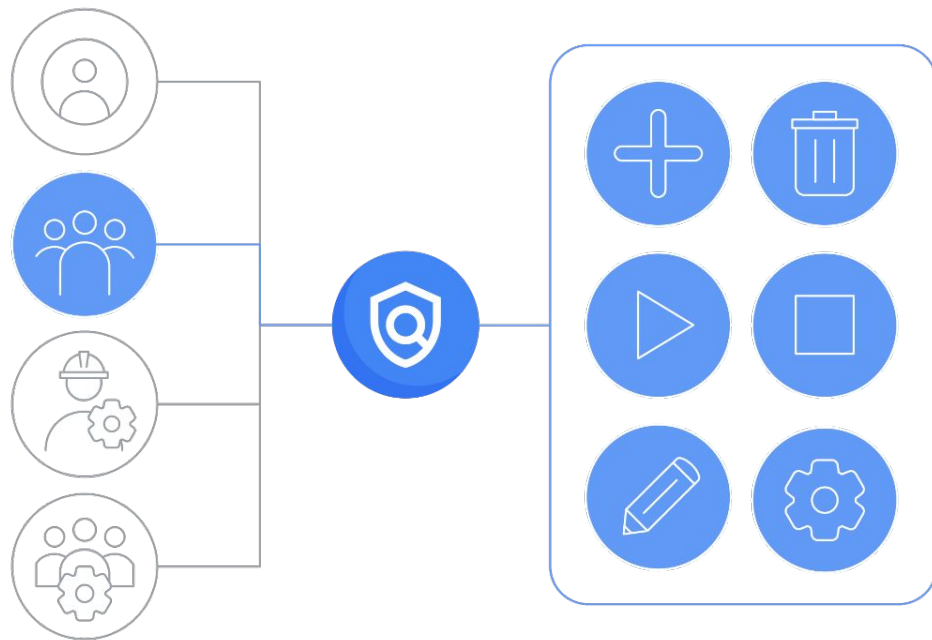
?

III

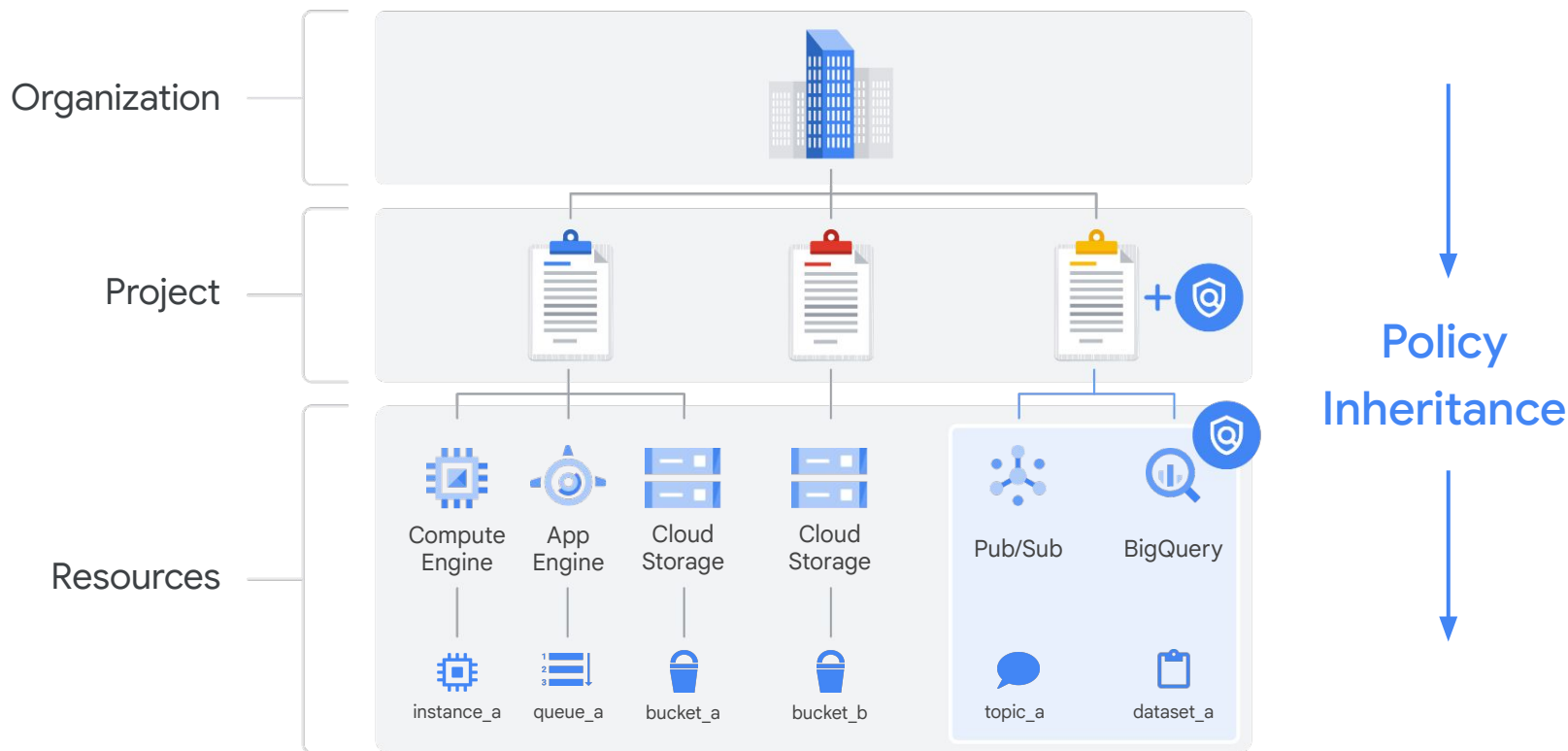
Type	Principal ↑	Name	Role	Security insights ?	
☐		630329882835-compute@developer.gserviceaccount.com	Compute Engine default service account	Editor	8765/8768 excess permissions
			Eventarc Event Receiver		
☐		cloud-apps-demos-w24@appspot.gserviceaccount.com	App Engine default service account	Editor	8768/8768 excess permissions
☐		erik.fredericks@gmail.com	Erik Fredericks	Owner	9813/9989 excess permissions

Identity and Access Management applies policies

Administrators can
apply policies that define
who can do **what** on
which resources



Policies are managed and applied by IAM

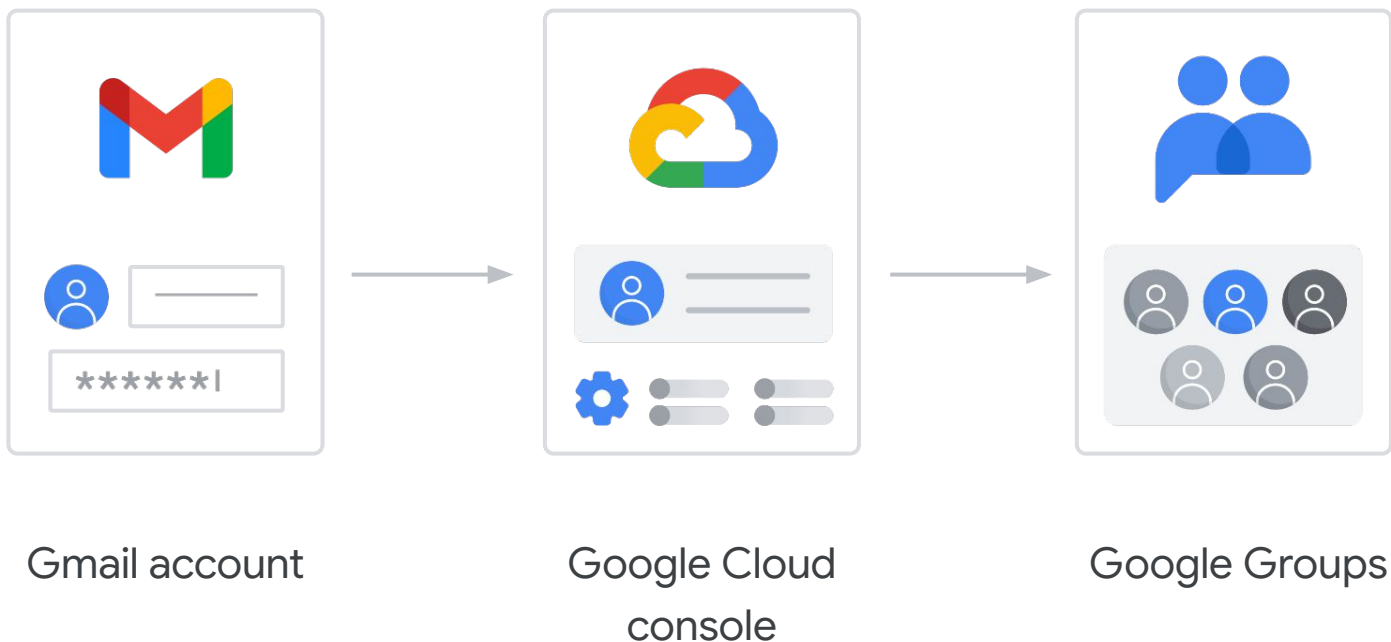


Deny policies prevent specific IAM permissions

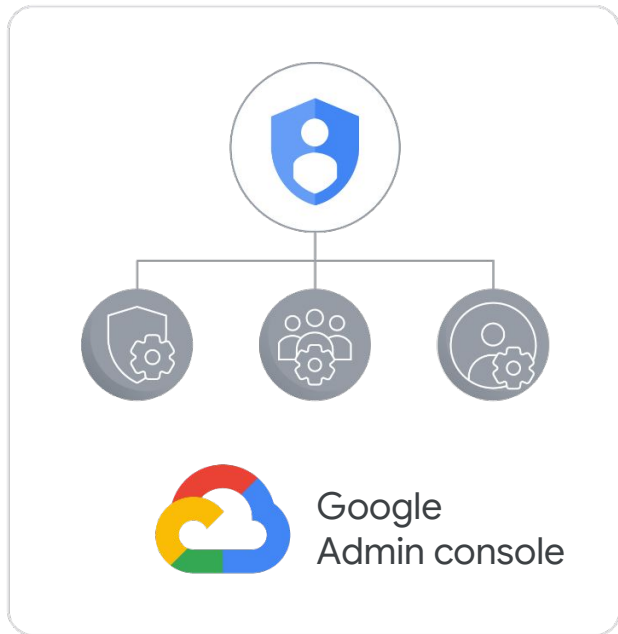
A **deny** policy overrides any existing **allow** policy regardless of the IAM role granted



Cloud Identity manages team and organization access



Cloud Identity defines user and group policies



With **Cloud Identity**, organizations can define policies and manage their users and groups using the **Google Admin console**



Cloud Identity



Log in and manage resources using the same credentials used in existing Active Directory or LDAP systems



The Google Admin console can be used to disable user accounts and remove them from groups when they leave



Available in free and premium editions



Already available to Google Workspace customers in the Google Admin console

There are three kinds of IAM roles

Basic
IAM role



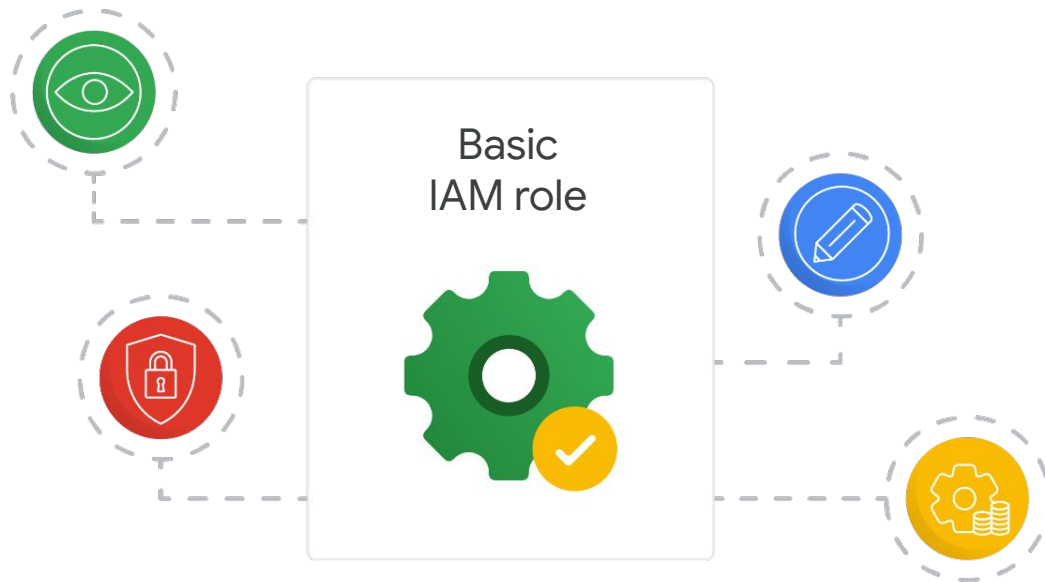
Predefined
IAM role



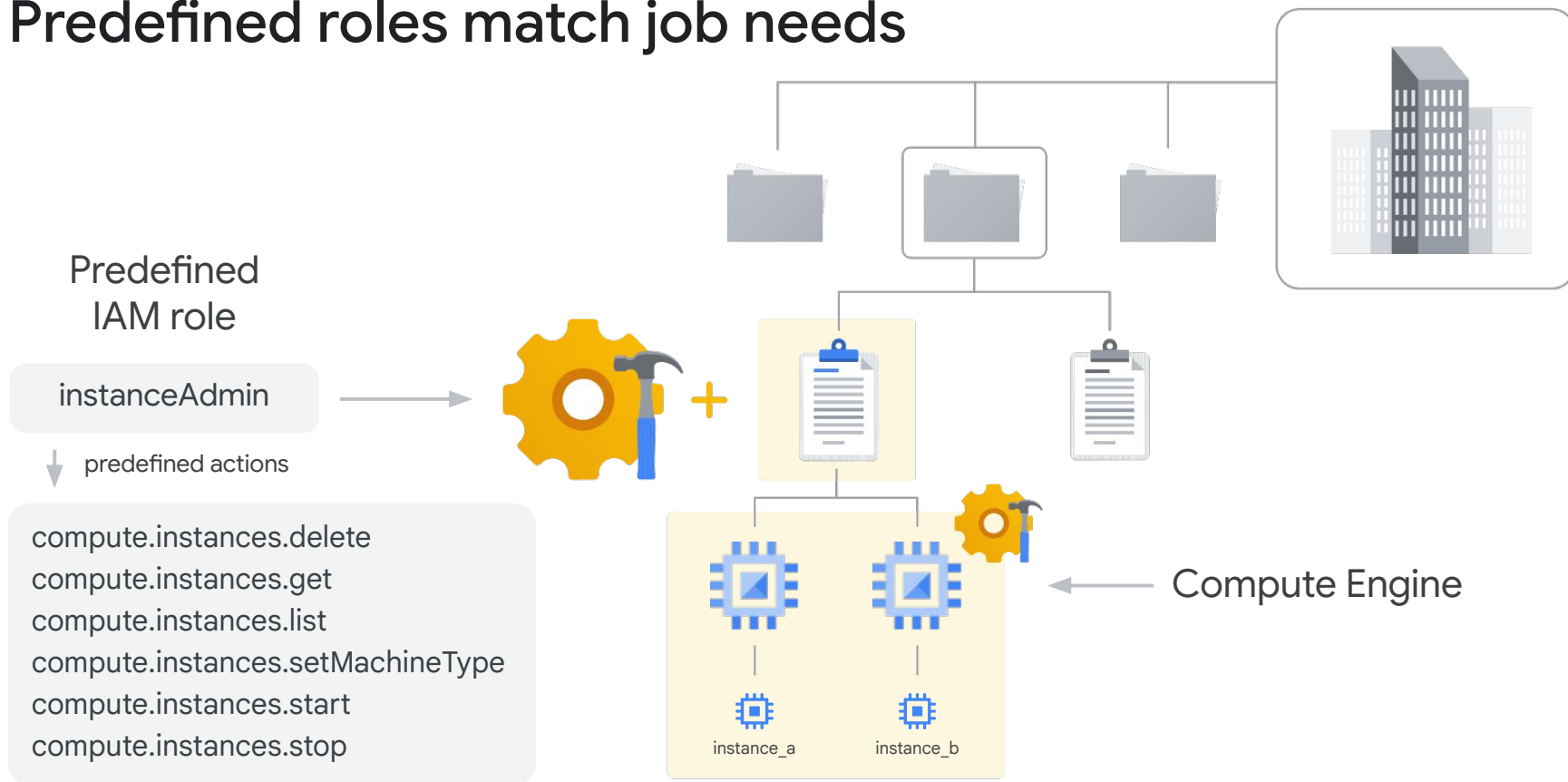
Custom
IAM role



Basic IAM roles are broad in scope



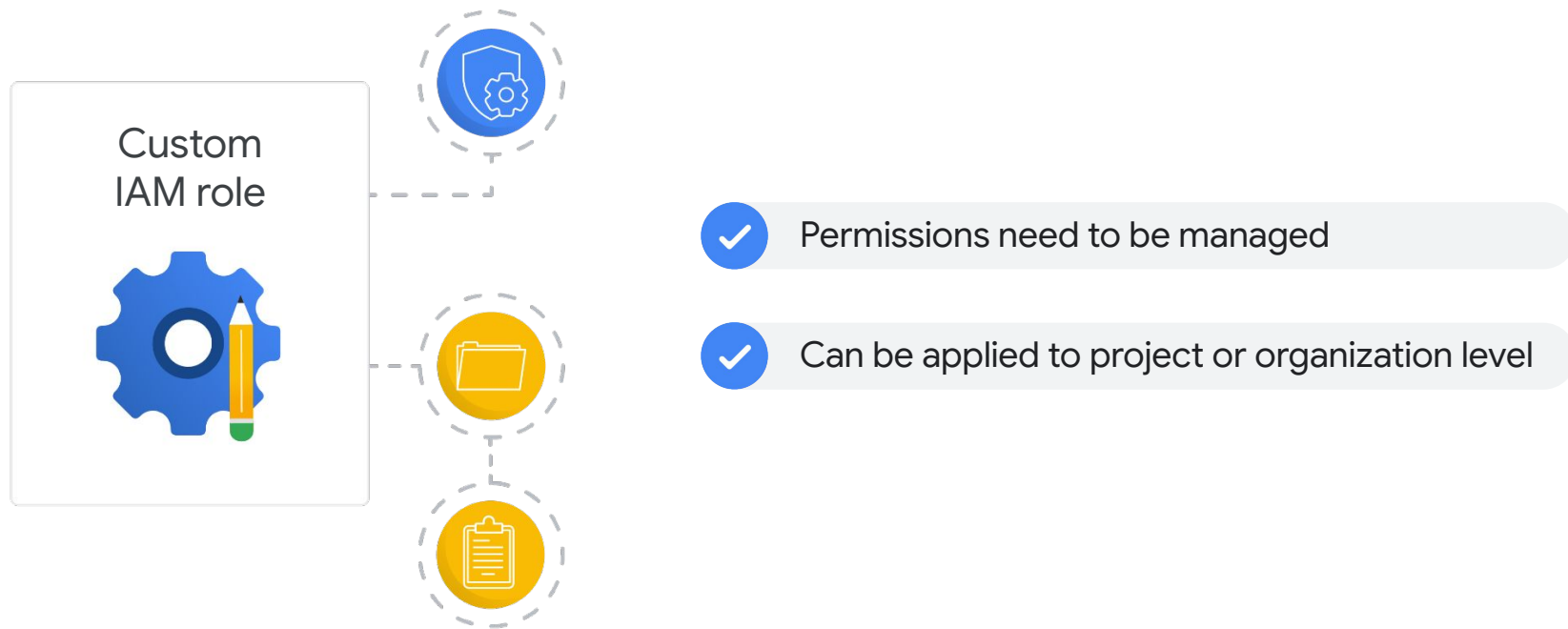
Predefined roles match job needs



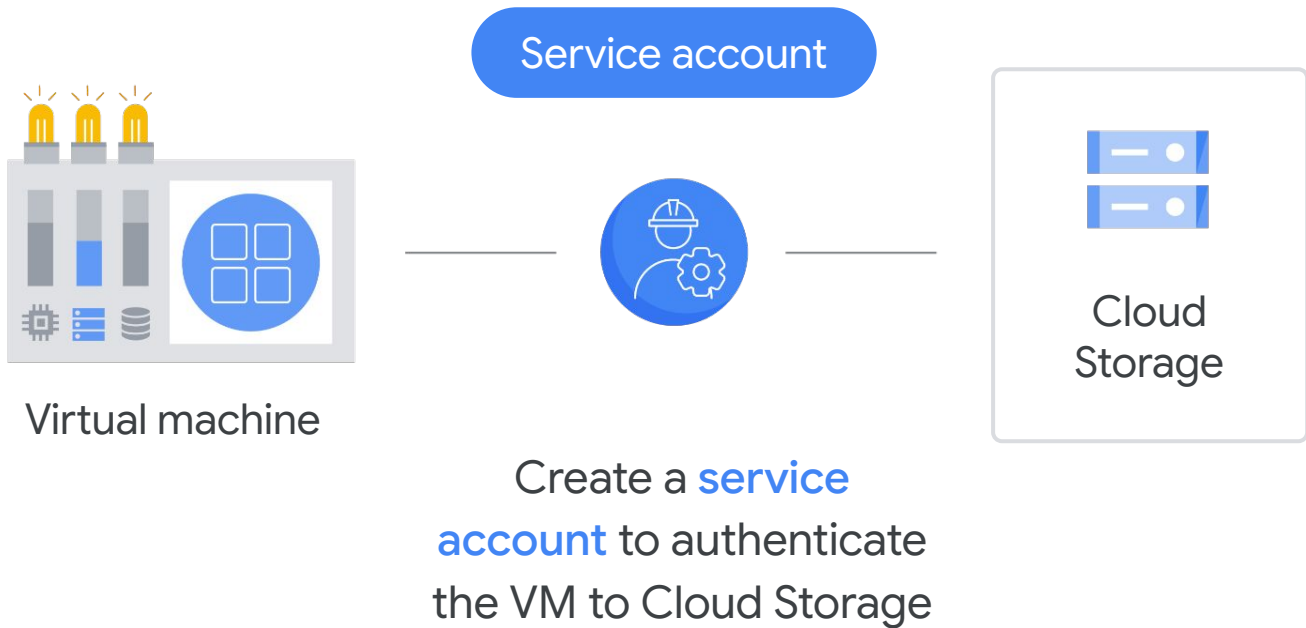
Custom roles are more specific and flexible



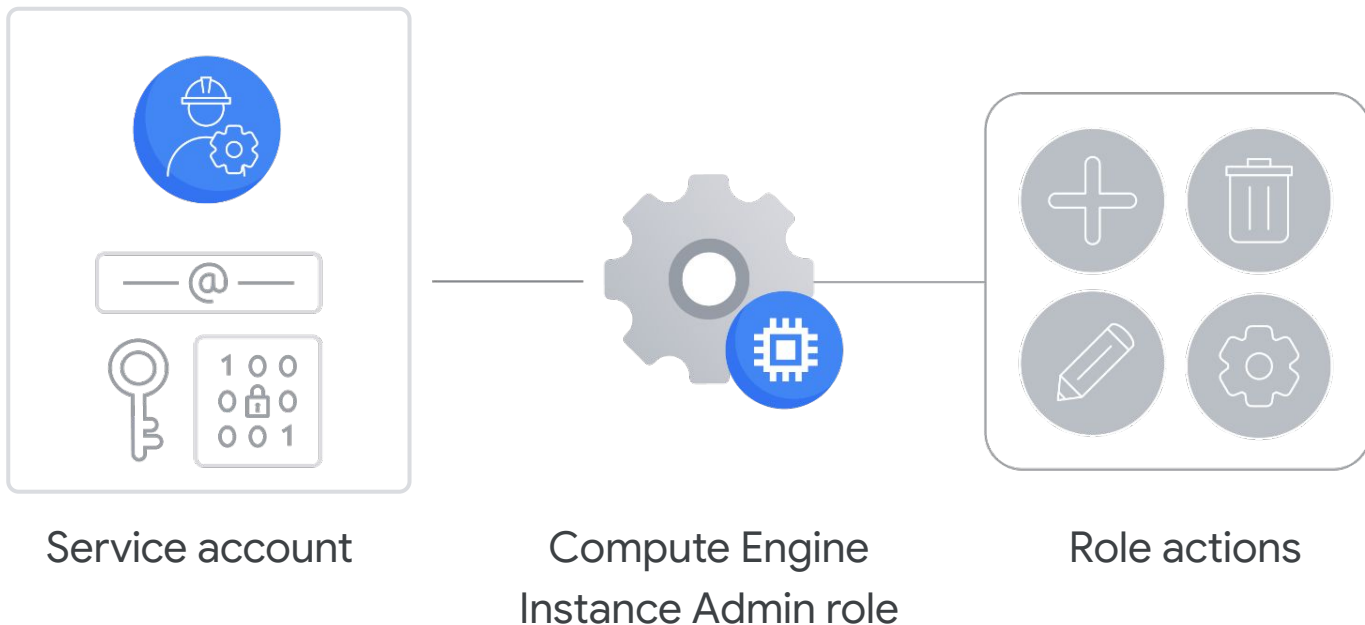
Custom roles are applied to projects and organizations



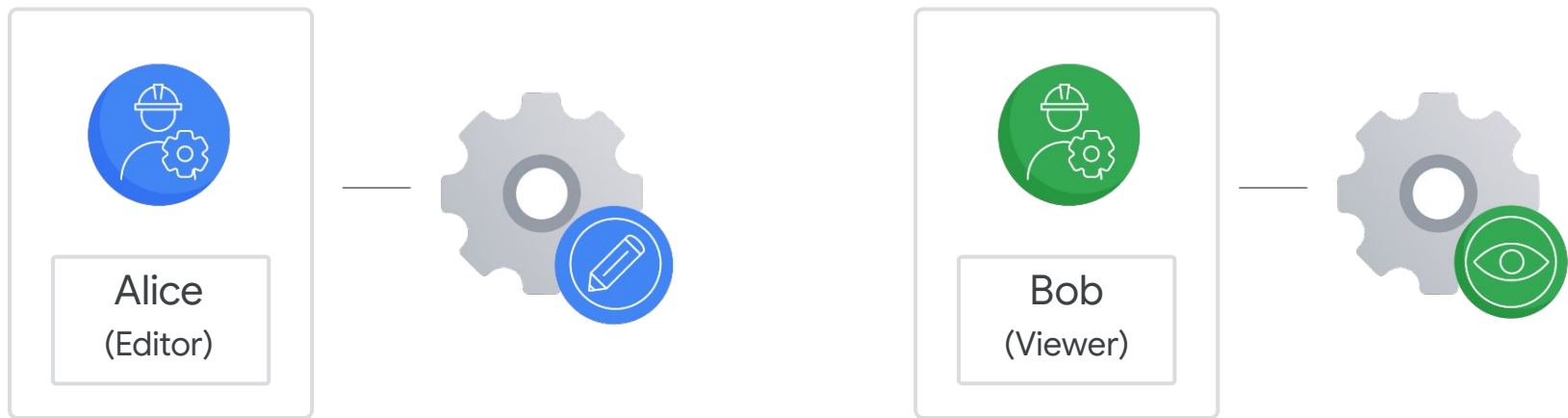
Permissions can be applied to service accounts



Service accounts are identified with email addresses



Service accounts are also managed by IAM



Cloud Skill!

<https://www.cloudskillsboost.google/focuses/5562?parent=catalog>

User Authentication: Identity-Aware Proxy

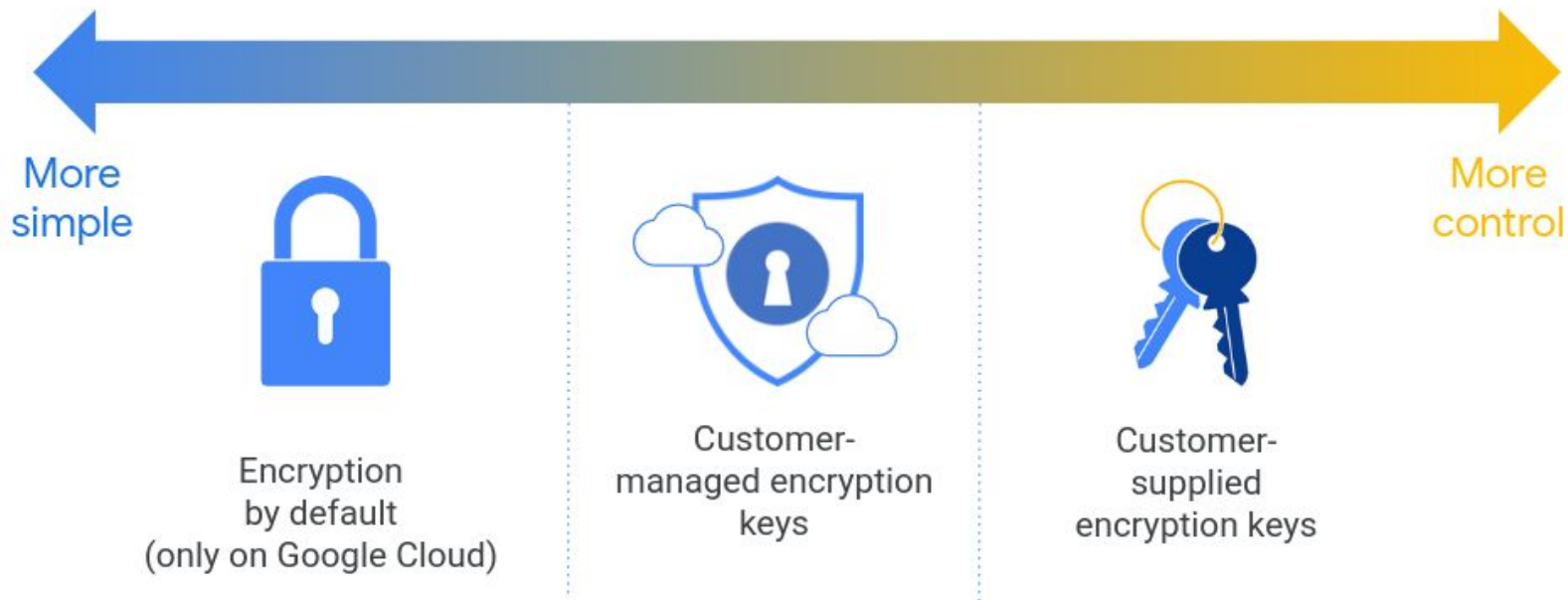
(was getting errors verifying app deployment)

Encryption

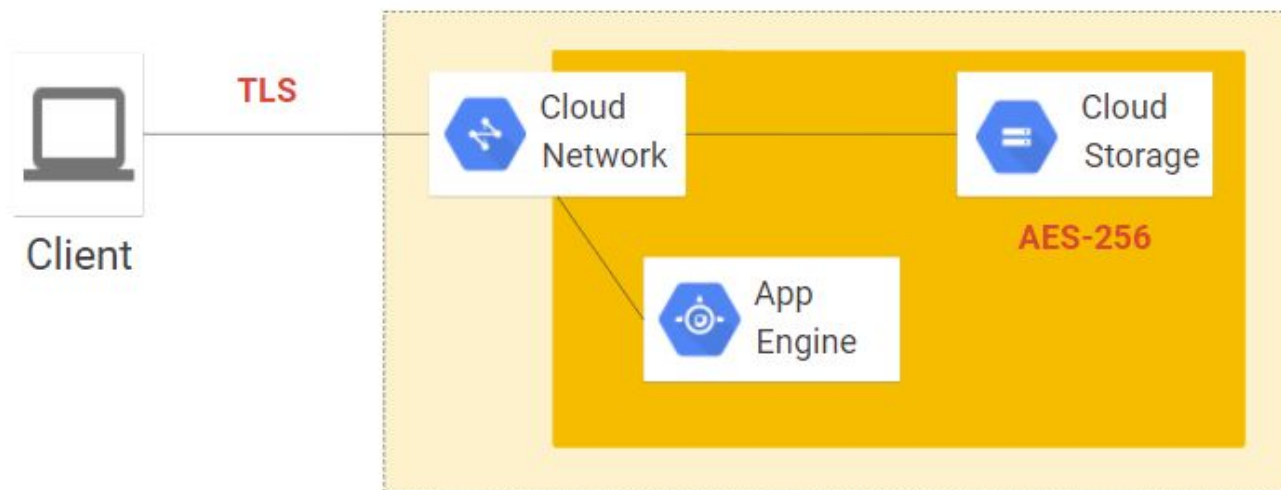
Goes hand-in-hand with security/privacy

- What is encryption?
- What techniques do you know?
- What is the difference between HTTP and HTTPS?

There are several encryption options



Google Cloud provides server-side encryption



Your options (in Google)

Traffic encrypted **by default**

- Though, if you choose to set things up without it that is still possible
 - e.g., a VM hosting an app that just sends data in cleartext

Customer-managed encryption keys (CMEK)

- Uses key management service (KMS):
<https://cloud.google.com/security-key-management>

Customer-supplied encryption keys (CSEK)

- Managed by you

CMEK

Cloud KMS - Google Cloud service for managing key-related activities such as:

- Encryption and decryption
- Signing certificates
- Data verification
- ... among others

CSEK

You generate and manage keys by yourself

- Pros/cons here?

You send keys to Google

- Use with their services

CMEK or CSEK

How do you choose?

Do you manage the keys yourself (CSEK)?

Do you let Google manage the keys (CMEK)?

Answer is "it depends"

- *and if you had me for 350, you'll lovingly remember that phrase*

KMS demo

<https://codelabs.developers.google.com/codelabs/encrypt-and-decrypt-data-with-cloud-kms#0>

Uses Cloud KMS to manage keys and **key rotation**

- What is rotation?

Best practices

Group resources with Projects

- i.e., sandboxing your environments and setting up "walls" around resources

Check policies **for each resource**

- Does some resource unintentionally inherit a security role from something else?
- e.g., is a private VM exposing a port? or is a public Cloud Function using a private storage bucket?

Best practices

Use the **principle of least privilege**

- Give resources the **minimal** amount of access needed to function
 - No more, no less

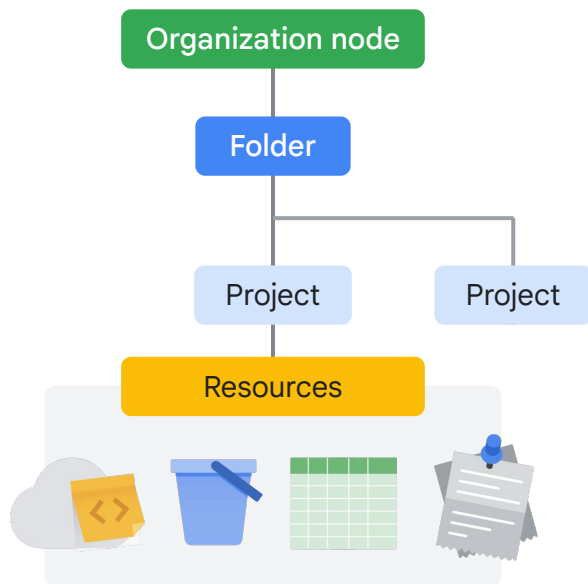
Routinely audit your policies

- Has something changed from the cloud provider?
- Did an intern accidentally open something up to the world?
- Did another developer introduce an inheritance issue?

Routinely monitor your logs

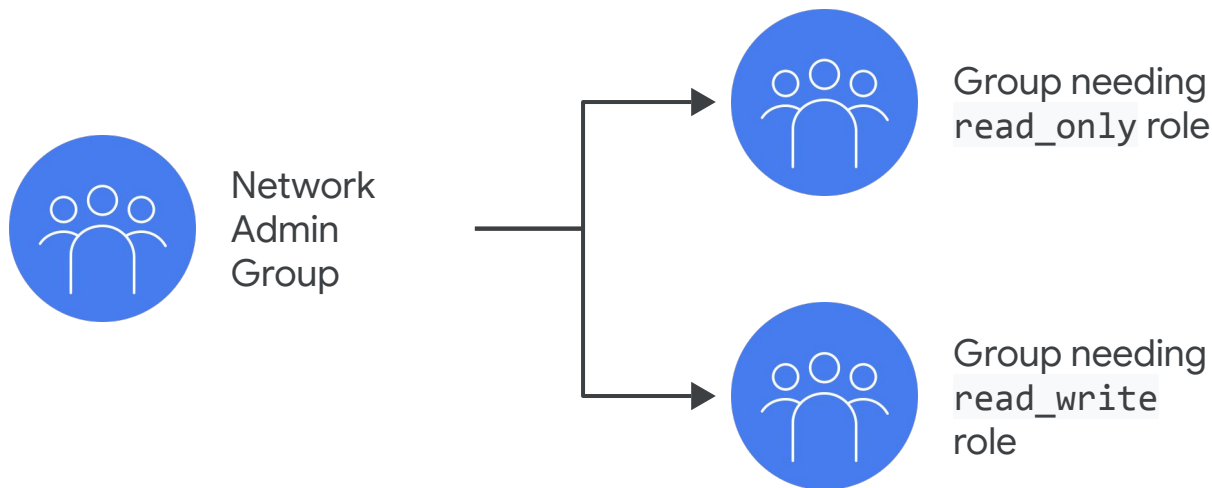
- Did somebody access your data that should be protected?
- Was a Cloud Function triggered 1,000,000,000 times instead of 1,000?

Leverage and understand the resource hierarchy

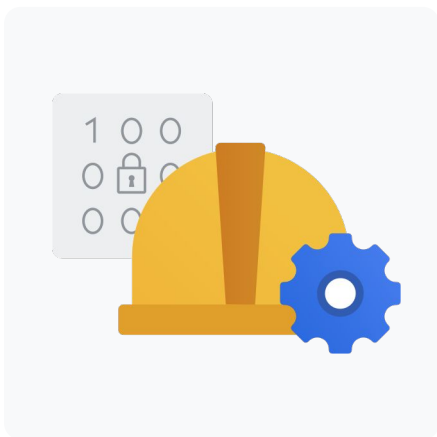


- ✓ Use projects to group resources
- ✓ Check the policy granted on each resource
- ✓ Use "principle of least privilege"
- ✓ Audit policies using Cloud Audit Logs
- ✓ Audit memberships of groups used in policies

Grant roles to groups instead of individuals



Best practices for service accounts



Use caution when granting the `serviceAccountUser` role.



Give a service account a display name that clearly identifies its purpose.



Establish a naming convention for service accounts.



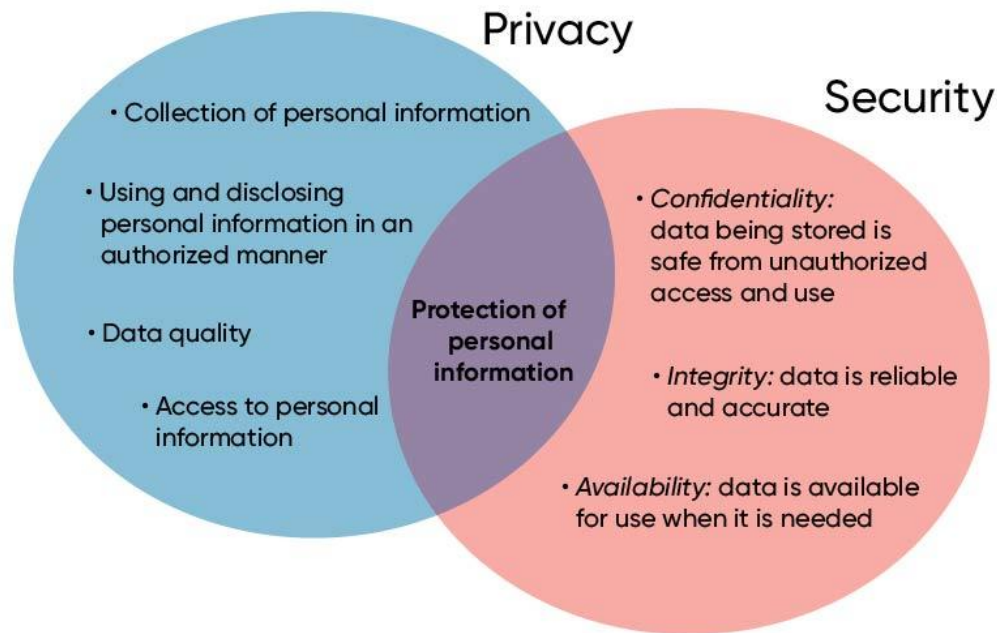
Establish key rotation policies and methods.

Privacy

What is the difference between security and privacy?

Privacy

What is the difference between security and privacy?



At present...

Nothing "specific" about privacy as that is **your responsibility**

However, guidelines!

<https://cloud.google.com/architecture/framework/security>

Considerations:

- Encrypting traffic
- Managing access
- GDPR!!!

In the security category of the Architecture Framework, you learn to do the following:

- [Review shared responsibility and shared fate on Google Cloud](#)
- [Understand security principles](#)
- [Manage risks with controls](#)
- [Manage your assets](#)
- [Manage identity and access](#)
- [Implement compute and container security](#)
- [Secure your network](#)
- [Implement data security](#)
- [Deploy applications security](#)
- [Manage compliance obligations](#)
- [Implement data residency and sovereignty requirements](#)
- [Implement privacy requirements](#)
- [Implement logging and detective controls](#)