Data Security and Industry Regulation

Target Complete Date	@December 16, 2022
Status	Completed
Reviewed	Reviewed
# Time to complete (Hours)	0.5
Type	Cloud Guru

💡 This is about the security of data and how it can be regulated in different industries.

⚙️ Data stored in GCP servers are encrypted.

Shared responsibility model

Principle of Least privelege

💡 Create service accounts with specific roles and permissions to reduce error.

Always be watching

💡 Audit logging and event threat detection. Always make sure you are monitoring who is accessing your data.

Data Security and Data Privacy

Regulatory complicance

> 💡 There may be strict laws regarding the type of data you are storing and how you need to handle it.

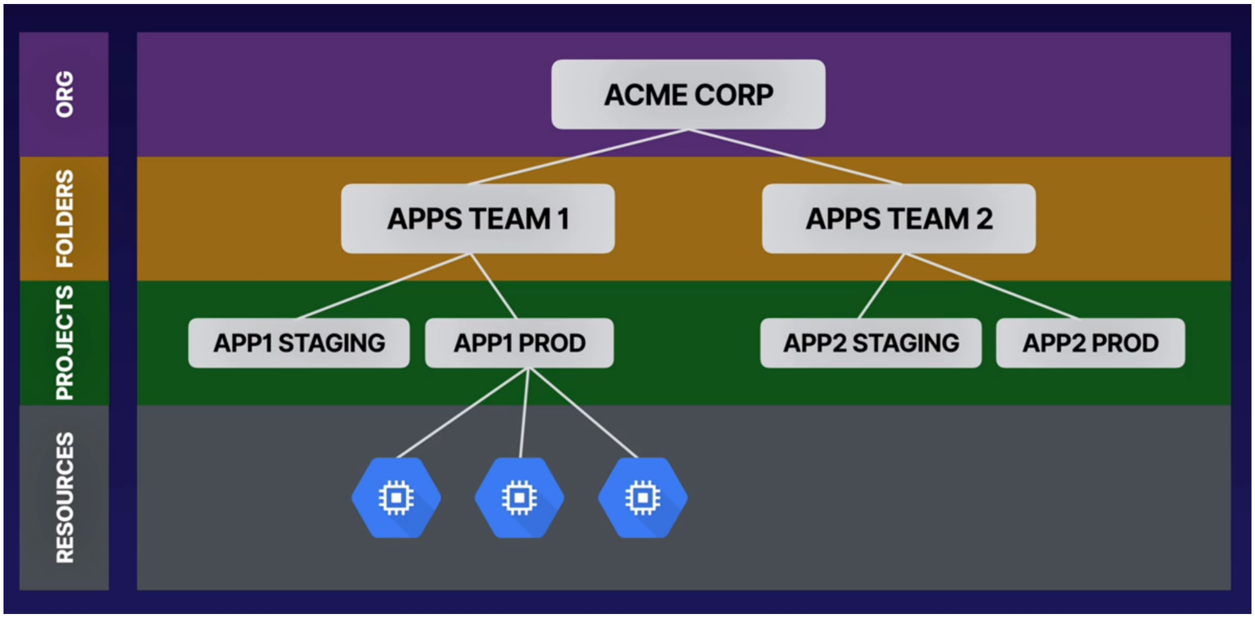
IAM best practices

The principle of Least privilege

> 💡 Use predefined role specific to each GCP product or service. You should view each application in the context of a trust boundary. The service should have precisely the permissions it needs to operate and nothing more. If it is compromised it won’t be able to access any others. This is known as limiting blast radius.

Hierarchy of access

1. Organization
2. Folders
3. Projects
4. Resources



💡 Childs can inherient policies from their parents.

Group access

💡 It is best practice to grant access to groups as opposed ot individual users. Such as a network admin group with the compute network role assigned to them.

Service accounts

💡 Special type of user account used by non human users. When you create a virtual machine it creates a service account to function. Programmatic access should also always be achieved through a service account. Service accounts are assigned IAM roles. Service accounts make use of keys for access. Keys should be rotated where possible.

> 💡 Create short lived credentials for service accounts where you can request OAUTH, OPENID or JWT tokens.

> 💡 Service account user role allows a user or service accounts to impersonate other service accounts.

Human users

> 💡 To access resources as a human account we use passwords and 2FA.

In production

> 💡 You should use the Cloud IAM API to audit your projects.

EXAM

> 💡 Learn the predefined IAM roles for each product and service.

Data Security

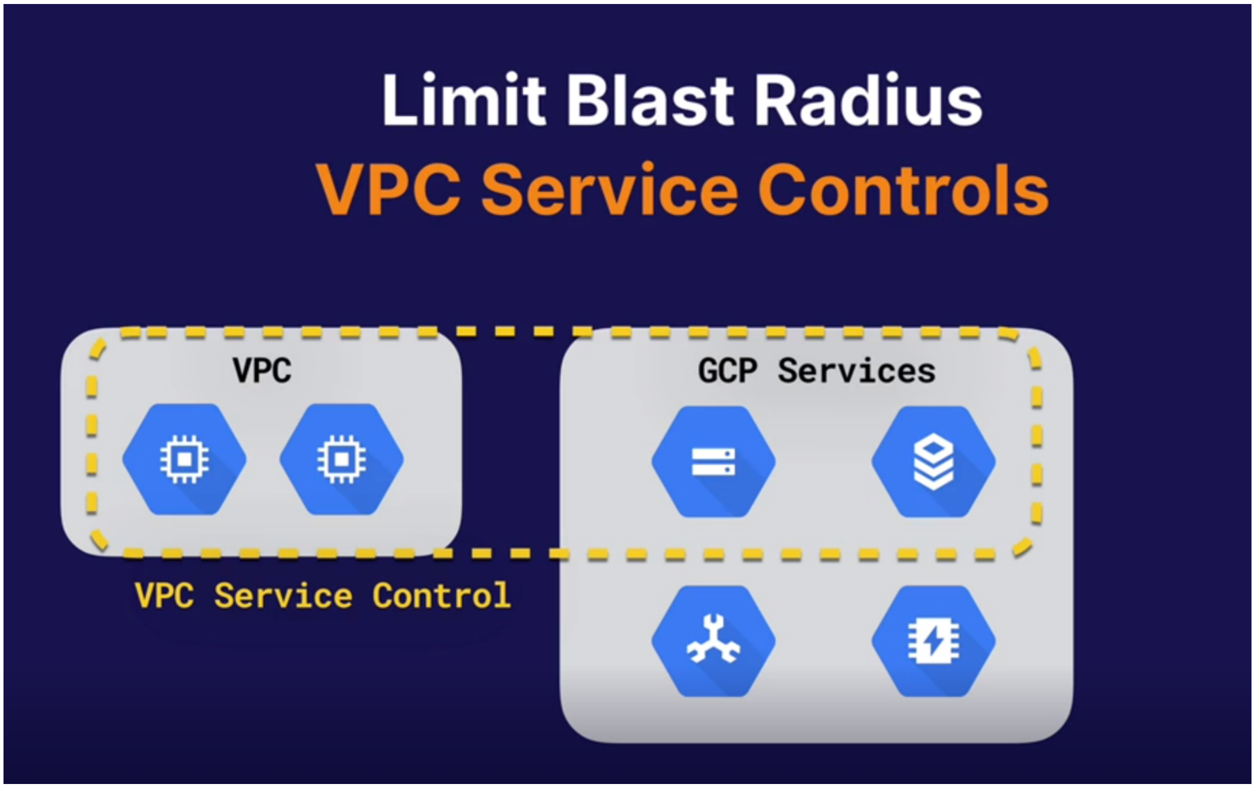
> 💡 Data is encrypted in flight and at rest for all data. You can also optionally choose to manage your own keys if you don’t trust googles.

Cloud Key management Service (KMS)

> 💡 This is a complete service for creating and managing your own keys in Google Cloud. Access to keys can be fully controlled via cloud IAM.

VPC service controls

> 💡 VPC service control can determine areas in which resources can contact eachother via VPCs. Resources within a VPC can contact other resources as long as they are in the same perimeter.



Limit Blast Radius

VPC Service Controls

GCP Security Command Center

☐ Look into this for exam

- Asset management
- Web secuirty Scanner
- Anomaly detection

- Threat detection

Data privacy

> 💡 Data security by itself may not be enough. You need to think about what is this data. Should you be storing it and who can access it?

Who can access the data?

> 💡 This is referring to having the authority to access and read sensitive data. The system itself may need to have row level encryption and authoritzation in place.

What is this data?

> 💡 What if the data contains PII data, or do we even need some of the data here.

GCP cloud data loss prevention API

> 💡 API to use in data pipelines to help remove or redact PII data. This works for text and image data, and it will use pseudo-anonymization to replace PII data with similarly formatted dummy data. As well as conduct risk analysis.

Industry regulation

FedRAMP (USA)

> 💡 Federal RIsk and Authorization Management program based in the USA. determins how data should be securely stored. It provides a stringint standards.

- High compliance for most GCP services

Children’s Online privacy protection Act (USA)

> 💡 Applicable to the collection of data for PII data for users under the age of 13. Based in the USA.

- Clear privacy policy
- Incorporate parent consent
- Justificaiton for any data collection

Health Insurance portability and accountability act (USA)

> 💡 Data security and privacy related to personal health information. Based in USA.

- Protects personal health information
- Requires acceptance of business associate agreement

PCI DDS (international)

> 💡 Payment card security standard across the globe. GCP is a platform that is secure enough for applications that store or process financial informaiton about credit cards.

General data protection regulation (EU)

> 💡 Designed to protect the personal data of european citizens.

- Applies to any company that interacts with the EU