

PRACTICE QUESTIONS

Google Cloud

Professional Cloud Security Engineer

SHARED BY [u/clever_socket_94](#) on aiexamcerts

EDITION Free Set 1

QUESTIONS 10

SHARED October 15, 2026

EXAM Google Cloud Professional Cloud Security Engineer

Shared by u/clever_socket_94 on aiexamcerts

10 practice questions for the Google Cloud Professional Cloud Security Engineer exam, each followed by its answer and a short explanation. More free sets and the full practice exam:

www.aiexamcerts.com/google-cloud/professional-cloud-security-engineer. Spotted a mistake? Email support@aiexamcerts.com with the exam name and the question number.

1. A security team wants to block creation of user-managed service account keys in a folder. Which mechanism applies this to every project beneath it?
 - A A Cloud Monitoring alert that notifies the security team whenever a key creation event is written to the audit logs
 - B An organization policy with the constraint iam.disableServiceAccountKeyCreation, set on the folder
 - C A Cloud Storage bucket policy that blocks key files
 - D A Terraform check that runs after each apply

Answer: B

The iam.disableServiceAccountKeyCreation constraint, set on the folder, prevents key creation in every project below it, so teams cannot switch it back on locally. An alert reports a key only after it has been created. Bucket policies and Terraform checks do not control service account key creation.

2. Access Context Manager defines access _____, which describe conditions such as IP ranges and device posture.

Answer: levels (also accepted: access levels)

An access level is a set of conditions that a request must meet, such as source IP ranges, device state or identity attributes. Access levels are referenced by policies such as Identity-Aware Proxy and VPC Service Controls. They do not grant permissions by themselves.

3. Which control stops sensitive data from leaving a defined boundary, even when a valid identity is used?
 - A Cloud Armor rate limiting rules for the public load balancer frontend
 - B A VPN tunnel with a static route
 - C A VPC Service Controls service perimeter
 - D Private Google Access on the subnet

Answer: C

A VPC Service Controls perimeter restricts API requests that cross its boundary, so data cannot be copied to a project outside the perimeter even by an authorized user. Rate limiting, VPN routing and Private Google Access do not enforce a data boundary for API calls. Identity alone is not enough to cross a perimeter.

4. Cloud KMS allows an administrator to view or extract the plaintext of a customer-managed key used by Cloud Storage.

- A True
- B False

Answer: B (False)

Cloud KMS does not reveal key material for customer-managed keys to administrators, because keys are used through cryptographic operations inside the service. Administrators can manage key lifecycle and permissions, but they cannot read the key itself. This property is central to customer control of encryption.

5. Which two actions protect data at rest in Cloud Storage? (Choose two.)

- A Use CMEK on the bucket so the customer controls the encryption key
- B Make the bucket public so it is easy to back up
- C Leave public access prevention turned off
- D Keep HMAC keys in a public Git repository
- E Rely on the default encryption that Google applies automatically

Answer: A, E

Cloud Storage encrypts data at rest by default, and CMEK adds customer control over the key. Public buckets, disabled public access prevention and keys in public repositories all expose data or its access credentials. Default encryption is not optional, so the default already protects data at rest.

6. Which approach protects a secret used by an application running on Cloud Run?

- A Store it as plain text in an environment variable baked into the container image at build time
- B Put it in a comment in the code
- C Commit it to the repository's README
- D Store it in Secret Manager and reference it at runtime with the runtime service account

Answer: D

Secret Manager stores the value with access controls and audit logs, and the runtime service account reads it when needed, so the secret stays out of code and images. A value baked into an image is visible to anyone who can pull it. Comments and READMEs are readable by everyone with repository access.

7. A security team must be alerted when a service account key is created in any project. Which control does this most directly?

- A A weekly manual review of IAM policies
- B A Cloud Logging log-based alert on the key creation audit event
- C A Cloud Armor rule
- D A Cloud DNS policy

Answer: B

A log-based alert matches the audit log entry for key creation and notifies the team as soon as it occurs. A weekly review finds the key days later, and Cloud Armor and DNS policies do not observe key creation at all. Pairing the alert with the disable-key-creation constraint covers both detection and prevention.

8. Security Health Analytics in Security Command Center detects _____, such as public buckets or open firewall rules.

Answer: misconfigurations

Security Health Analytics scans resource configuration against known risky settings and reports misconfigurations as findings. Those findings can be prioritized and assigned for remediation. Runtime threats are covered by Event Threat Detection instead.

9. Which control gives the organization advance notice and approval over Google staff access to its data?

- A Access Approval
- B Cloud Billing alerts for unusual spending
- C VPC flow logs
- D Cloud DNS

Answer: A

Access Approval sends the customer a request before Google personnel can access its content, and the customer can approve or deny it. Billing alerts track cost, flow logs record network traffic, and Cloud DNS resolves names. None of them gate staff access.

10. Which record proves that a deleted service account key was not used after a specific date?

- A A Cloud Billing invoice that lists the service account's charges for the month
- B Cloud Audit Logs for the service account, retained beyond the default period
- C A VM startup script
- D A DNS zone file

Answer: B

Audit logs record authentication and key activity with timestamps, so retained logs show the last use of the key and prove when use stopped. Invoices show charges, startup scripts run at boot, and DNS zone files list records. Only audit logs record the access history.