

PRACTICE QUESTIONS

Google Cloud

Professional Cloud Security Engineer

SHARED BY [u/Zesty-Lemur-3934](#) on aiexamcerts

EDITION Free Set 2

QUESTIONS 10

SHARED October 15, 2026

EXAM Google Cloud Professional Cloud Security Engineer

Shared by [u/Zesty-Lemur-3934](#) 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. An auditor asks who read a sensitive BigQuery table. Which audit log type answers this?

- A Admin Activity logs, which are the only logs needed for reads
- B Platform logs for Compute Engine instances
- C Data Access audit logs, which record reads and writes of user data
- D Access Transparency logs

Answer: C

Data Access audit logs record API calls that read or write user data, so they show which principal read the table. Admin Activity logs record configuration changes rather than data reads. Access Transparency logs record actions by Google staff, not by the customer's own administrators.

2. An IAM Deny policy applies only to basic roles, leaving predefined roles unaffected.

- A True
- B False

Answer: B (False)

IAM Deny policies can block specific permissions regardless of which role grants them, including predefined roles. This is why deny policies are useful for guardrails. Restricting them to basic roles would make them far less effective.

3. A security administrator must allow only images signed by a trusted attester to be deployed to Cloud Run and GKE. Which control applies?

- A A Cloud Armor edge policy
- B A Cloud DNS allowlist
- C A Private Service Connect endpoint that routes traffic to the registry over private addresses
- D Binary Authorization policy with attestations from a trusted attester

Answer: D

Binary Authorization checks each image at deployment against a policy, and a policy can require attestations from named attestors. Cloud Armor filters web traffic, and DNS allowlists do not verify image signatures. Private Service Connect provides private network paths, which is a different problem from image trust.

4. Cloud Armor Adaptive Protection uses machine learning to detect and suggest rules for _____ attacks at the application layer.

Answer: DDoS (also accepted: layer 7 DDoS)

Adaptive Protection analyzes traffic patterns to spot application-layer, or layer 7, DDoS attacks and suggests rules to block them. It complements static rules and preconfigured WAF protections. Its suggestions can be reviewed before they are applied.

5. Which two steps improve incident response readiness? (Choose two.)

- A Write and rehearse playbooks for common security events
- B Delete old logs as soon as they are created to save space
- C Keep audit logs for only one day
- D Give every responder Owner rights on all projects
- E Pre-approve a forensic snapshot procedure for affected VMs

Answer: A, E

Rehearsed playbooks let responders act correctly under pressure, and pre-approved forensic procedures let them preserve evidence without waiting for approvals. Deleting logs or keeping them for a day removes the evidence that investigations need. Owner rights on every project give responders far more access than an incident requires.

6. A bucket must keep objects for seven years and block their deletion, even by administrators. Which feature does this?

- A A bucket retention policy with Bucket Lock
- B Object versioning, turned on with a lifecycle rule that deletes old versions after thirty days
- C Uniform bucket-level access
- D Public access prevention

Answer: A

A retention policy sets the minimum age before objects can be deleted, and locking it makes the policy permanent, so it cannot be shortened or removed. Versioning keeps old copies but does not stop deletion, and the lifecycle rule would delete the versions anyway. Access settings control who can read, not how long objects are kept.

7. Analysts need a dataset, but social security numbers must not be visible to them. Which control fits?
- A Give analysts Owner access so they can manage the dataset themselves without waiting for an administrator
 - B Column-level security using BigQuery policy tags on the sensitive column
 - C Share the full table and ask analysts not to query the column
 - D Export the table as a public CSV file

Answer: B

Policy tags in BigQuery restrict access to specific columns, so analysts without the fine-grained reader role cannot see the sensitive values. Asking people not to query a column is not an enforced control. Owner access and public exports widen exposure rather than limiting it.

8. Access Transparency records actions taken by Google staff when they access customer data.
- A True
 - B False

Answer: A (True)

Access Transparency logs record when Google personnel access customer content for support or operations, along with the reason. Customers can review these logs. Pairing them with Access Approval lets the customer control such access.

9. Which approach lets an organization show it can respond to a GDPR data deletion request?
- A Keeping all personal data forever in case it is needed later
 - B Storing deletion requests in an email inbox that is checked now and then
 - C A documented process with tooling to find and delete the subject's data across every store
 - D Telling users to delete their own accounts and data

Answer: C

A documented process with tooling to locate and delete a person's data across systems shows the organization can meet the request within the required time. Keeping data indefinitely conflicts with storage limitation, and an inbox does not track completion. Asking users to delete their own data does not discharge the organization's obligation.

10. A regulator wants proof that a specific administrator changed a firewall rule. Which evidence is best?
- A A verbal confirmation from the administrator
 - B A screenshot of the console taken today
 - C An IAM policy listing the administrator's role
 - D Cloud Audit Logs entries that show the firewall change with the principal and timestamp

Answer: D

Audit log entries record the principal, the method, the resource and the time of the change, which is verifiable and retained independently of the people involved. A verbal confirmation or a screenshot can be disputed. An IAM policy shows what the administrator could do, not what they did.