

[Google Discussions](#)

Exam Professional Cloud Security Engineer All Questions

View all questions & answers for the Professional Cloud Security Engineer exam

[Go to Exam](#)

EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 289 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 289

Topic #: 1

[\[All Professional Cloud Security Engineer Questions\]](#)

You work for an organization that handles sensitive customer data. You must secure a series of Google Cloud Storage buckets housing this data and meet these requirements:

- Multiple teams need varying access levels (some read-only, some read-write).
- Data must be protected in storage and at rest.
- It's critical to track file changes and audit access for compliance purposes.
- For compliance purposes, the organization must have control over the encryption keys.

What should you do?



- A. Create IAM groups for each team and manage permissions at the group level. Employ server-side encryption and Object Versioning by Google Cloud Storage. Configure cloud monitoring tools to alert on anomalous data access patterns.
- B. Set individual permissions for each team and apply access control lists (ACLs) to each bucket and file. Enforce TLS encryption for file transfers. Enable Object Versioning and Cloud Audit Logs for the storage buckets.
- C. Use predefined IAM roles tailored to each team's access needs, such as Storage Object Viewer and Storage Object User. Utilize customer-supplied encryption keys (CSEK) and enforce TLS encryption. Turn on both Object Versioning and Cloud Audit Logs for the storage buckets.
- D. Assign IAM permissions for all teams at the object level. Implement third-party software to encrypt data at rest. Track data access by using network logs.

[Show Suggested Answer](#)

Comments

Type your comment...

Submit

  **Pime13** 7 months, 3 weeks ago

Selected Answer: C

This approach ensures that:


Access Control: IAM roles are tailored to each team's needs, providing the principle of least privilege.

Data Protection: Customer-supplied encryption keys (CSEK) give your organization control over encryption keys, and TLS encryption protects data in transit.

Compliance and Auditing: Object Versioning and Cloud Audit Logs help track file changes and audit access for compliance purposes.

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

   upvoted 1 times

  **Pime13** 7 months, 3 weeks ago

<https://cloud.google.com/monitoring/compliance/data-at-rest>

<https://cloud.google.com/blog/products/storage-data-transfer/google-cloud-storage-best-practices-to-help-ensure-data-privacy-and-security>

   upvoted 1 times

  **KLei** 8 months, 2 weeks ago

Selected Answer: C

By utilizing CSEK, your organization maintains control over the encryption keys, which is crucial for compliance purposes.

   upvoted 2 times

  **yokoyan** 10 months, 3 weeks ago




Selected Answer: C

I think it's C.

   upvoted 3 times

  **json4u** 9 months, 2 weeks ago

I agree. Only C satisfies all requirements above.

   upvoted 2 times



Platform

> Home

> Examtopics PRO

> All Exams

> Training Courses



