

 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 219 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 219

Topic #: 1

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

You are migrating an on-premises data warehouse to BigQuery, Cloud SQL, and Cloud Storage. You need to configure security services in the data warehouse. Your company compliance policies mandate that the data warehouse must:

- Protect data at rest with full lifecycle management on cryptographic keys.
- Implement a separate key management provider from data management.
- Provide visibility into all encryption key requests.

What services should be included in the data warehouse implementation? (Choose two.)

- A. Customer-managed encryption keys
- B. Customer-Supplied Encryption Keys
- C. Key Access Justifications
- D. Access Transparency and Approval
- E. Cloud External Key Manager




[Show Suggested Answer](#)

by  gcp4test at Aug. 4, 2023, 3:01 p.m.

Comments

Type your comment...

Submit




  **gcp4test** Highly Voted  1 year, 11 months ago

Selected Answer: CE

Implement a separate key management provider from data management - so the key must be outside of the GCP - E

Provide visibility into all encryption key requests. - this can be supported by - C

   upvoted 5 times

  **ArizonaClassics** Highly Voted  1 year, 11 months ago

C. Key Access Justifications

Key Access Justifications can provide visibility into all encryption key requests, satisfying your third condition. This feature enables you to get justification for every request to use a decryption key, giving you the information you need to decide whether to approve or deny the request in real-time.

E. Cloud External Key Manager

The Cloud External Key Manager allows you to use and manage encryption keys stored outside of Google's infrastructure, thereby providing a separate key management provider from data management. This meets your first and second conditions because it enables you to fully manage the lifecycle of your cryptographic keys while storing them outside Google Cloud.

   upvoted 5 times

  **YourFriendlyNeighborhoodSpider** Most Recent  4 months, 1 week ago

Selected Answer: AE

AE looks correct, many people in the comments explained why, take a note.

   upvoted 1 times

  **7f97f9f** 5 months, 1 week ago

Selected Answer: AE

A. CMEK allows you to control the encryption keys used to protect your data at rest. You have full control over the key lifecycle. This is a crucial component.

C. KAJ requires that Google support personnel provide a justification for accessing customer content. It does not provide visibility into all encryption key requests.

E. Cloud EKM allows you to use encryption keys that are managed in an external key management system (KMS) that you control. This fulfills the requirement of separating key management from data management. This also provides visibility into key requests, as they are being requested from your external KMS.

Therefore the answer is A. and E.

   upvoted 2 times

  **p981pa123** 6 months, 1 week ago

Selected Answer: AE

A and E

   upvoted 1 times

  **BPzen** 8 months ago

Selected Answer: AE

Why Option A (Customer-Managed Encryption Keys) is Correct
Control Over Keys:

Customer-managed encryption keys (CMEK) allow you to manage the lifecycle of encryption keys, including rotation, revocation, and deletion, through Cloud Key Management Service (KMS).
Integration with BigQuery, Cloud SQL, and Cloud Storage:

CMEK is supported across BigQuery, Cloud Storage, and Cloud SQL, enabling encryption of data at rest with your managed keys.

Compliance Support:

CMEK satisfies the requirement to manage the full lifecycle of encryption keys.

   upvoted 1 times

  **Betotoxicity** 1 year, 3 months ago

Selected Answer: AE

Why not C?: KAJ focuses on managing access control for Google personnel to resources, not specifically on encryption key visibility

visibility.

   upvoted 1 times

  **Betotoxicity** 1 year, 3 months ago

Selected Answer: CE

Why not C?: KAJ focuses on managing access control for Google personnel to resources, not specifically on encryption key visibility.

   upvoted 1 times

  **adb4007** 1 year, 5 months ago

Selected Answer: CE

CE seems good for me.

If you want to be compliance with "Implement a separate key management provider from data management" you must have 2 providers and "B" CSEK couldn't work i think. "E" work for the both first policies. "C" seems good for the third policy.

   upvoted 2 times

  **cyberpunk21** 1 year, 11 months ago

Selected Answer: CE

looks good to me

   upvoted 2 times


  **anshad666** 1 year, 11 months ago

Selected Answer: CE

C - <https://cloud.google.com/assured-workloads/key-access-justifications/docs/overview>

E - <https://cloud.google.com/kms/docs/ekm>

   upvoted 2 times

  **STomar** 1 year, 11 months ago

AE:

<https://cloud.google.com/kms/docs/cmek>

A: CMEK gives you control over the keys that protect your data at rest in Google Cloud. Using CMEK gives you control over more aspects of the lifecycle and management of your keys.

   upvoted 1 times

  **akg001** 1 year, 11 months ago

Selected Answer: CE

C,E - looks correct to me

   upvoted 3 times

  **Sanjana2020** 1 year, 11 months ago

I think this is BE. They mention that they want the data and the keys to be in separate locations. So that would mean CSEK. And that is handled by External Key Manager. So BE.

   upvoted 2 times



Platform

> Home

> Examtopics PRO

> All Exams

> Training Courses



