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 287 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 287
Topic #: 1
[All Professional Cloud Security Engineer Questions]

You work for a banking organization. You are migrating sensitive customer data to Google Cloud that is currently encrypted at rest while on-premises. There are strict regulatory requirements when moving sensitive data to the cloud. Independent of the cloud service provider, you must be able to audit key usage and be able to deny certain types of decrypt requests. You must choose an encryption strategy that will ensure robust security and compliance with the regulations. What should you do?

A. Utilize Google default encryption and Cloud IAM to keep the keys within your organization's control.

B. Implement Cloud External Key Manager (Cloud EKM) with Access Approval, to integrate with your existing on-premises key management solution.

C. Implement Cloud External Key Manager (Cloud EKM) with Key Access Justifications to integrate with your existing one premises key management solution.

D. Utilize customer-managed encryption keys (CMEK) created in a dedicated Google Compute Engine instance with Confidential Compute encryption, under your organization's control.

Show Suggested Answer

by yokoyan at *Sept. 6, 2024, 1:51 a.m.*

Comments

Type your comment...

Submit

json4u Highly Voted 9 months, 2 weeks ago

Answer is C.
- Access Approval : This lets you control access to your organization's data by Google personnel.
- Key Access Justifications : This provides a justification for every request to access keys stored in an external key manager.

upvoted 5 times

Pime13 Most Recent 7 months, 3 weeks ago

Selected Answer: C

https://cloud.google.com/kms/docs/ekm#terminology
https://cloud.google.com/assured-workloads/key-access-justifications/docs/overview
Key Access Justifications

When you use Cloud EKM with Key Access Justifications, each request to your external key management partner includes a field that identifies the reason for each request. You can configure your external key management partner to allow or deny requests based on the Key Access Justifications code provided.

upvoted 1 times

MoAk 8 months, 1 week ago

Selected Answer: C

Answer is C. https://cloud.google.com/kms/docs/ekm#terminology

upvoted 2 times

KLei 8 months, 2 weeks ago

Selected Answer: B

C does not offer the same level of access control as Access Approval, which is critical for denying unauthorized decrypt requests.

upvoted 1 times

dv1 9 months, 1 week ago

Selected Answer: C

Key Access Justifications does what the question asks for.

upvoted 3 times

yokoyan 10 months, 3 weeks ago

Selected Answer: B

I think it's B.

upvoted 2 times