

[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 259 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 259

Topic #: 1

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

Your team maintains 1PB of sensitive data within BigQuery that contains personally identifiable information (PII). You need to provide access to this dataset to another team within your organization for analysis purposes. You must share the BigQuery dataset with the other team while protecting the PII. What should you do?


- A. Utilize BigQuery's row-level access policies to mask PII columns based on the other team's user identities.
- B. Export the BigQuery dataset to Cloud Storage. Create a VPC Service Control perimeter and allow only their team's project access to the bucket.
- C. Implement data pseudonymization techniques to replace the PII fields with non-identifiable values. Grant the other team access to the pseudonymized dataset.
- D. Create a filtered copy of the dataset and replace the sensitive data with hash values in a separate project. Grant the other team access to this new project.

[Show Suggested Answer](#)

by  yokoyan at Sept. 6, 2024, 1:26 a.m.

### Comments

[Submit](#)

  **Pime13** 7 months, 3 weeks ago

**Selected Answer: C**

Why Option C?


Data Protection: Pseudonymization replaces PII with non-identifiable values, ensuring that sensitive information is protected while still allowing the other team to perform their analysis.

Compliance: This approach helps in complying with data protection regulations by minimizing the risk of exposing PII.

Usability: The other team can access and analyze the dataset without compromising the privacy of the individuals whose data is included

Why not A?

   upvoted 1 times

  **LegoJesus** 5 months, 3 weeks ago


The question starts with "Your team maintains 1 Peta Byte of data in bigquery".  
That's a lot of data.

If you go with option C, you either:

- De-identify the sensitive information in the original dataset, rendering this table and the info in it useless for the original team that uses it.
- Clone the entire dataset (another 1PB), de-identify the sensitive data and grant access to the other team.

So obviously A is the better answer here, because the PII is still needed, just can't share it with other teams.

   upvoted 1 times

  **Pime13** 7 months, 3 weeks ago



Option A suggests using BigQuery's row-level access policies to mask PII columns based on the other team's user identities.

Granularity of Protection: Row-level access policies are useful for controlling access to specific rows based on user identities, but they may not be as effective for masking or protecting specific columns containing PII. This approach might not fully anonymize the data, leaving some sensitive information potentially exposed.




Complexity and Maintenance: Implementing and maintaining row-level access policies can be complex, especially if the dataset is large and the access requirements are detailed. This can lead to increased administrative overhead.


Pseudonymization Benefits: Pseudonymization (option C) ensures that PII is replaced with non-identifiable values, providing a higher level of data protection. This method is more straightforward and ensures that the other team can work with the data without risking exposure of sensitive information.

   upvoted 1 times

  **Pime13** 7 months, 3 weeks ago

<https://cloud.google.com/blog/products/identity-security/how-to-use-google-cloud-to-find-and-protect-pii>  
<https://cloud.google.com/sensitive-data-protection/docs/dlp-bigquery>


   upvoted 1 times

  **cachopo** 7 months, 3 weeks ago

**Selected Answer: A**

Option A is the best approach because it allows you to implement fine-grained, secure access directly within BigQuery without needing to duplicate or transform the dataset. By using row-level access policies and column masking, you can efficiently protect the PII while enabling the other team to analyze the non-sensitive portions of the data.

   upvoted 1 times

  **nah99** 8 months ago

**Selected Answer: A**

A.

<https://cloud.google.com/bigquery/docs/row-level-security-intro>

   upvoted 1 times

  **KLei** 8 months, 2 weeks ago

**Selected Answer: A**

A provides less footprint to solve the problem.

   upvoted 1 times

  **jmaquino** 8 months, 2 weeks ago

**Selected Answer: A**

Example: [https://cloud.google.com/bigquery/docs/row-level-security-intro?hl=es-419#filter\\_row\\_data\\_based\\_on\\_region](https://cloud.google.com/bigquery/docs/row-level-security-intro?hl=es-419#filter_row_data_based_on_region)

   upvoted 2 times

  **jmaquino** 8 months, 2 weeks ago

**Selected Answer: A**

Sorry: A: I disagree with answer C. Row-level security allows you to filter data and enable access to specific rows in a table, based on eligible user conditions. Row-level security allows a data owner or administrator to implement policies, such as

based on eligible user conditions. Row-level security allows a data owner or administrator to implement policies, such as "Team Users." <https://cloud.google.com/bigquery/docs/row-level-security-intro?hl=en-US>

👍 ↩ 🚩 upvoted 2 times

🗄 👤 **KLei** 8 months, 2 weeks ago

yes, "replace" the original data is wrong. we need somewhere to keep the true copy of data. If copy to another target and then replace the PII then it is OK. But saying 1PB data, it is time consuming for the copy operation and high BQ cost. C is not a good option.

👍 ↩ 🚩 upvoted 1 times

🗄 👤 **nah99** 8 months ago

True, they included the 1PB to make C blatantly worse

👍 ↩ 🚩 upvoted 1 times

🗄 👤 **jmaquino** 8 months, 2 weeks ago

**Selected Answer: C**

A: I disagree with answer C. Row-level security allows you to filter data and enable access to specific rows in a table, based on eligible user conditions. Row-level security allows a data owner or administrator to implement policies, such as "Team Users." <https://cloud.google.com/bigquery/docs/row-level-security-intro?hl=en-US>

👍 ↩ 🚩 upvoted 1 times

🗄 👤 **KLei** 8 months, 2 weeks ago

so your answer should be A. My answer is A

👍 ↩ 🚩 upvoted 1 times

🗄 👤 **yokoyan** 10 months, 3 weeks ago

**Selected Answer: C**

I think it's C.

👍 ↩ 🚩 upvoted 2 times

🗄 👤 **KLei** 8 months, 2 weeks ago

replacing the original PII values in the BQ? so where is the original true copy of data?

👍 ↩ 🚩 upvoted 1 times



## Platform

> Home

> All Exams

> Examtopics PRO

> Training Courses

