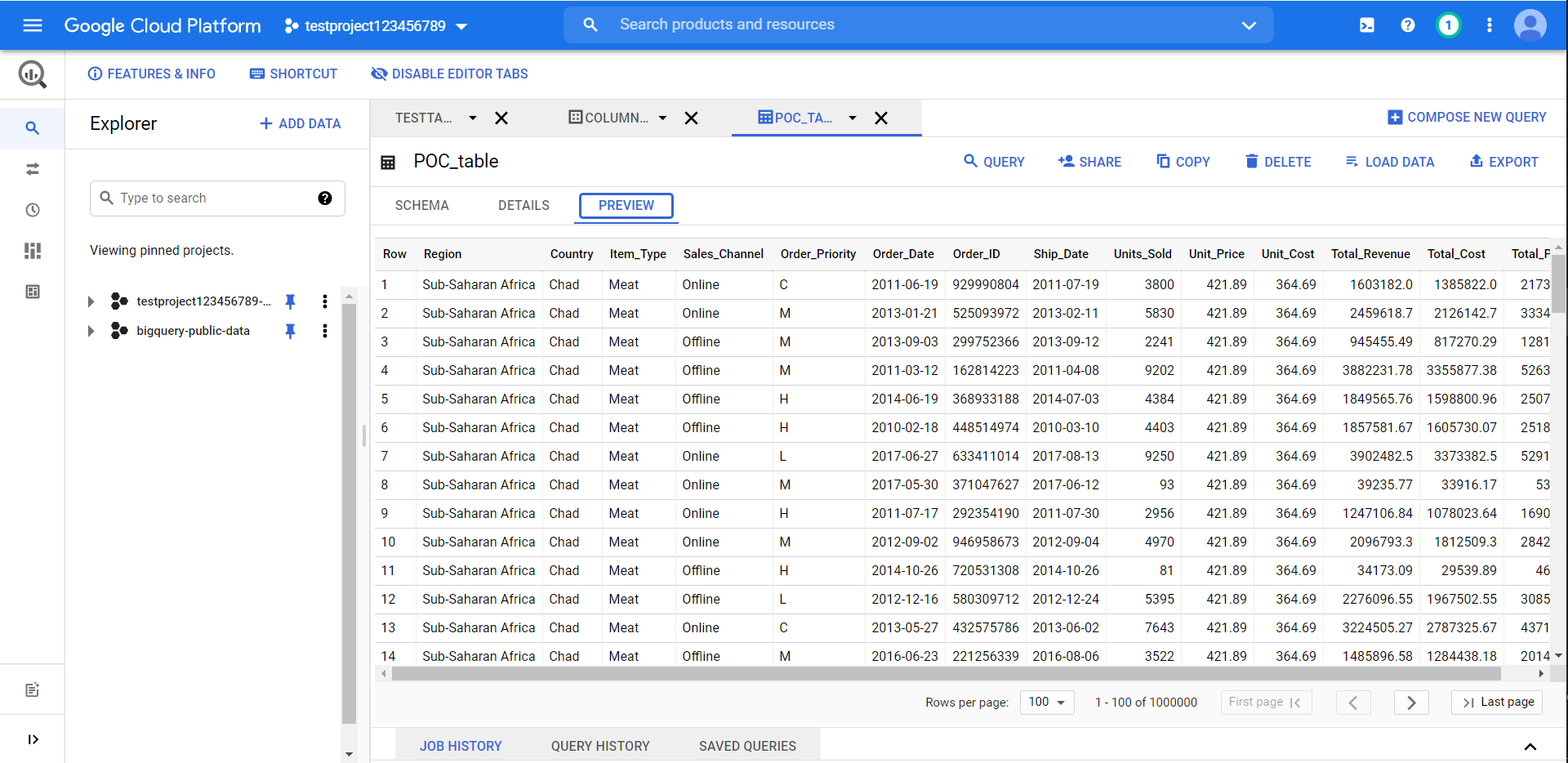
**Implementing Column-level security in BigQuery**

This document explains how to implement bigquery column-level security to restrict access to BigQuery data at column level.

GCP services to be used:

* BigQuery
* Data catalog

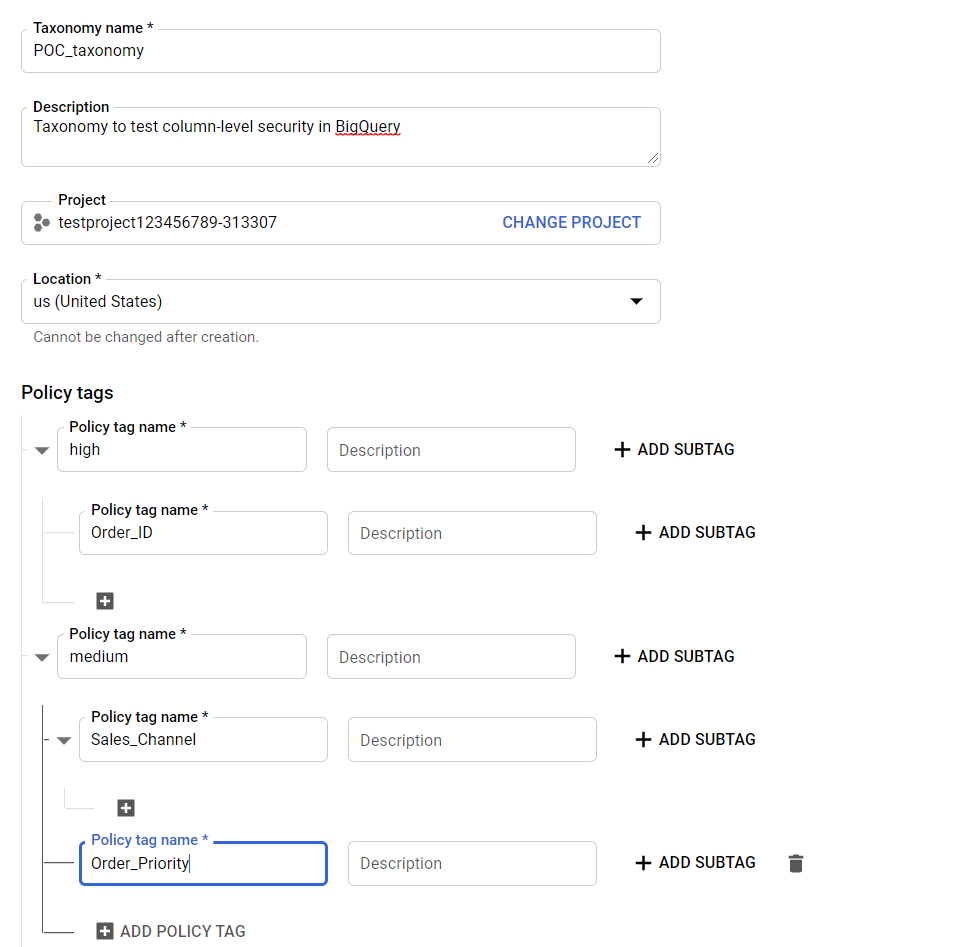
Sample Preview of the Table



Here we will be restricting access of Order\_ID through one policy tag and Sales\_Channel & Order\_Priority through other policy tag

Step 1: Create a taxonomy in Data Catalog

Open Data Catalog page in GCP -> Select Policy Tags -> Click Create taxonomy

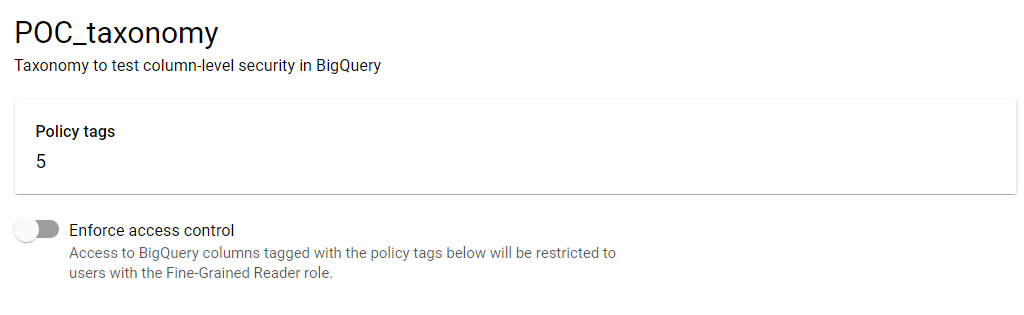


Set policy tags based on the nomenclature and add the column name whose access needs to be restricted as subtag.

Taxonomy region and region of BigQuery dataset must be the same.

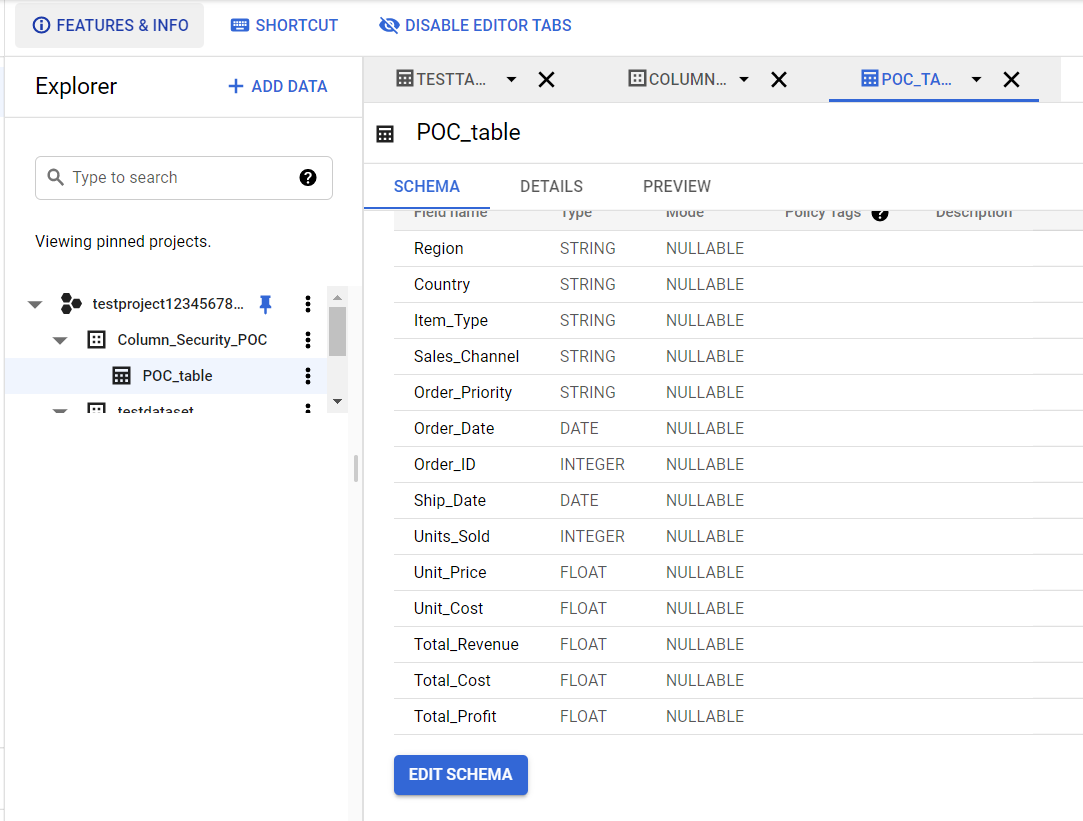
Click on Create

Step 2: Enable Enforce access control for the taxonomy

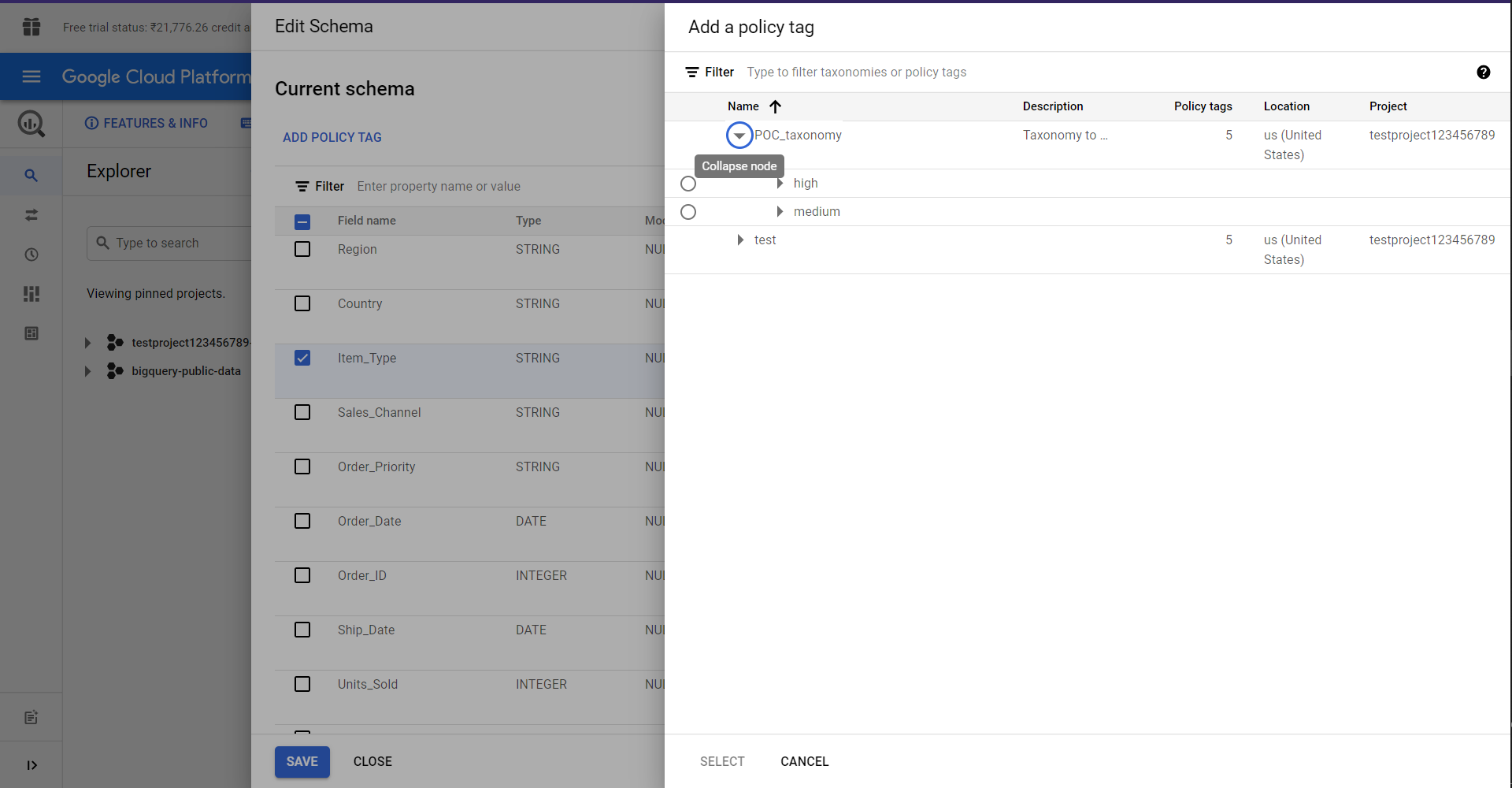


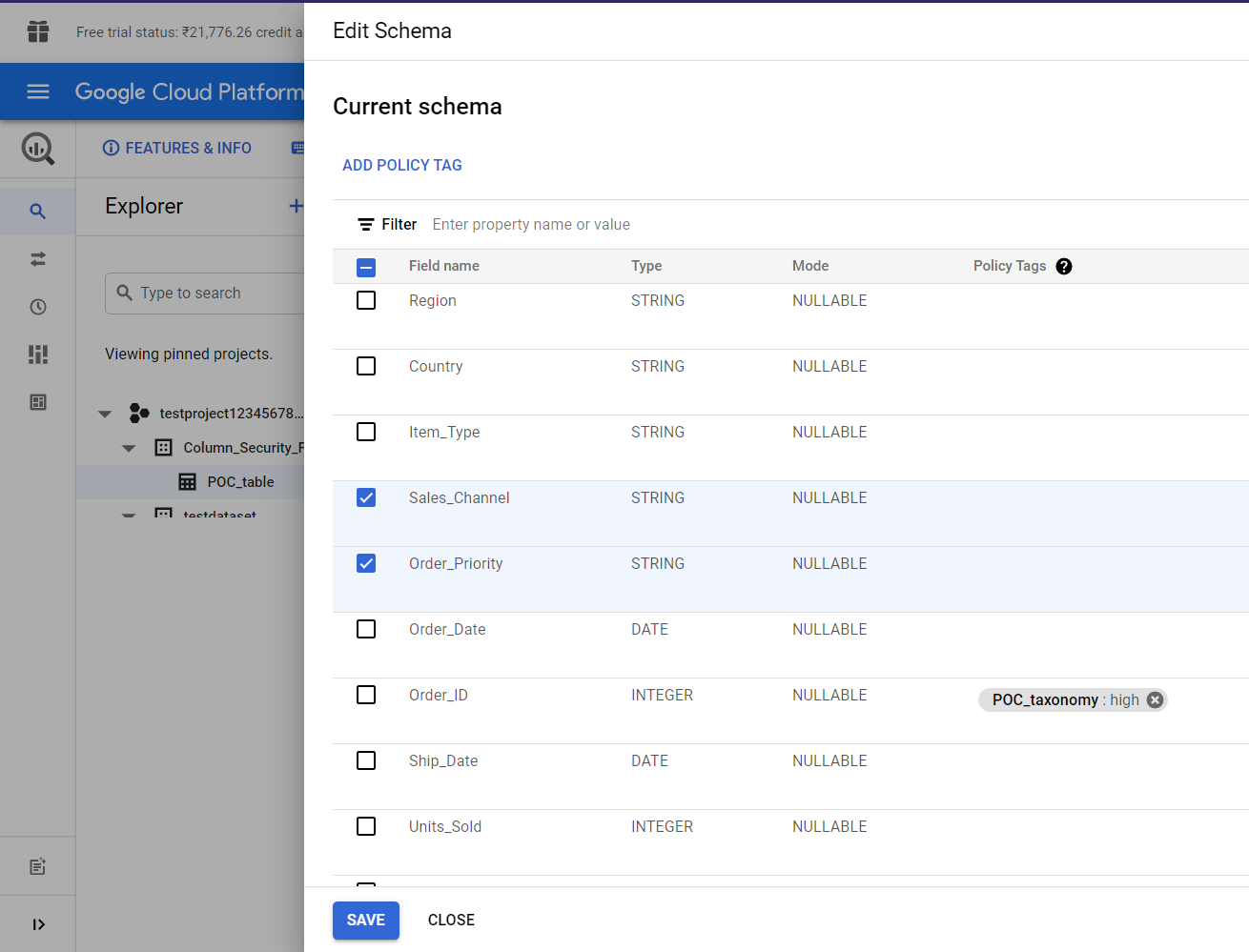
Step-3: Edit BigQuery Schema

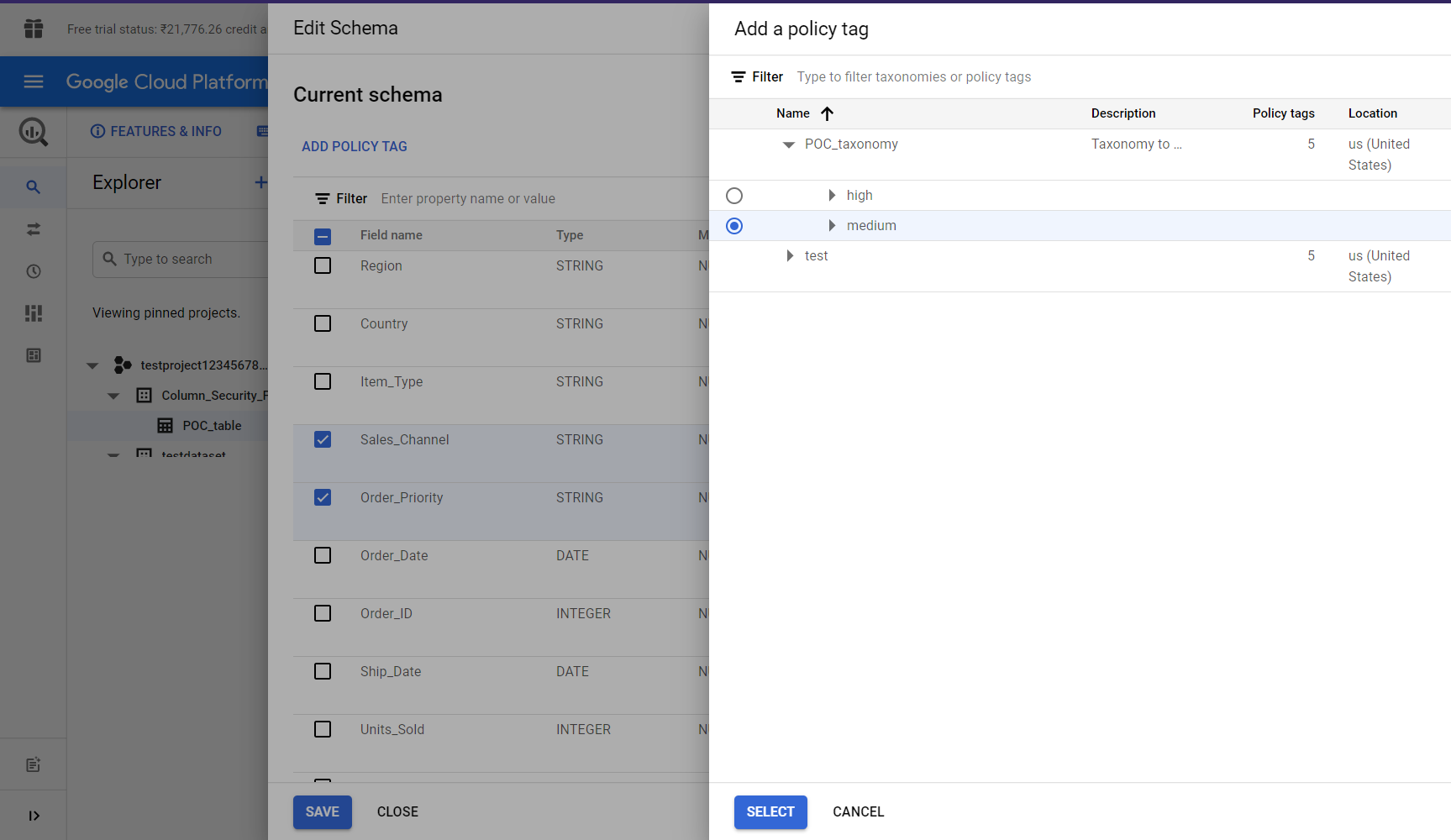
Select the table -> Select schema then click on edit schema

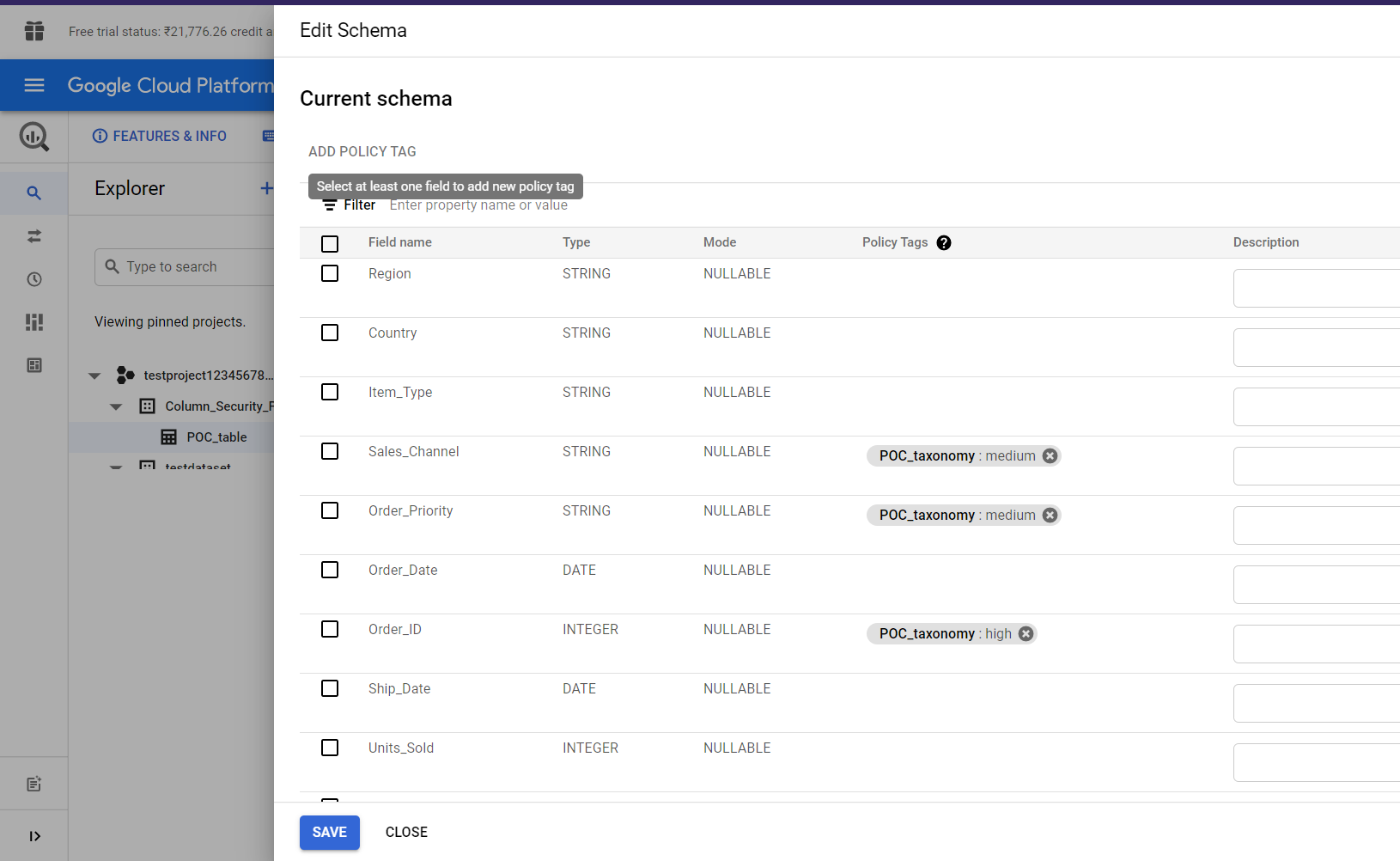


Select the specific columns and click on Add Policy Tags





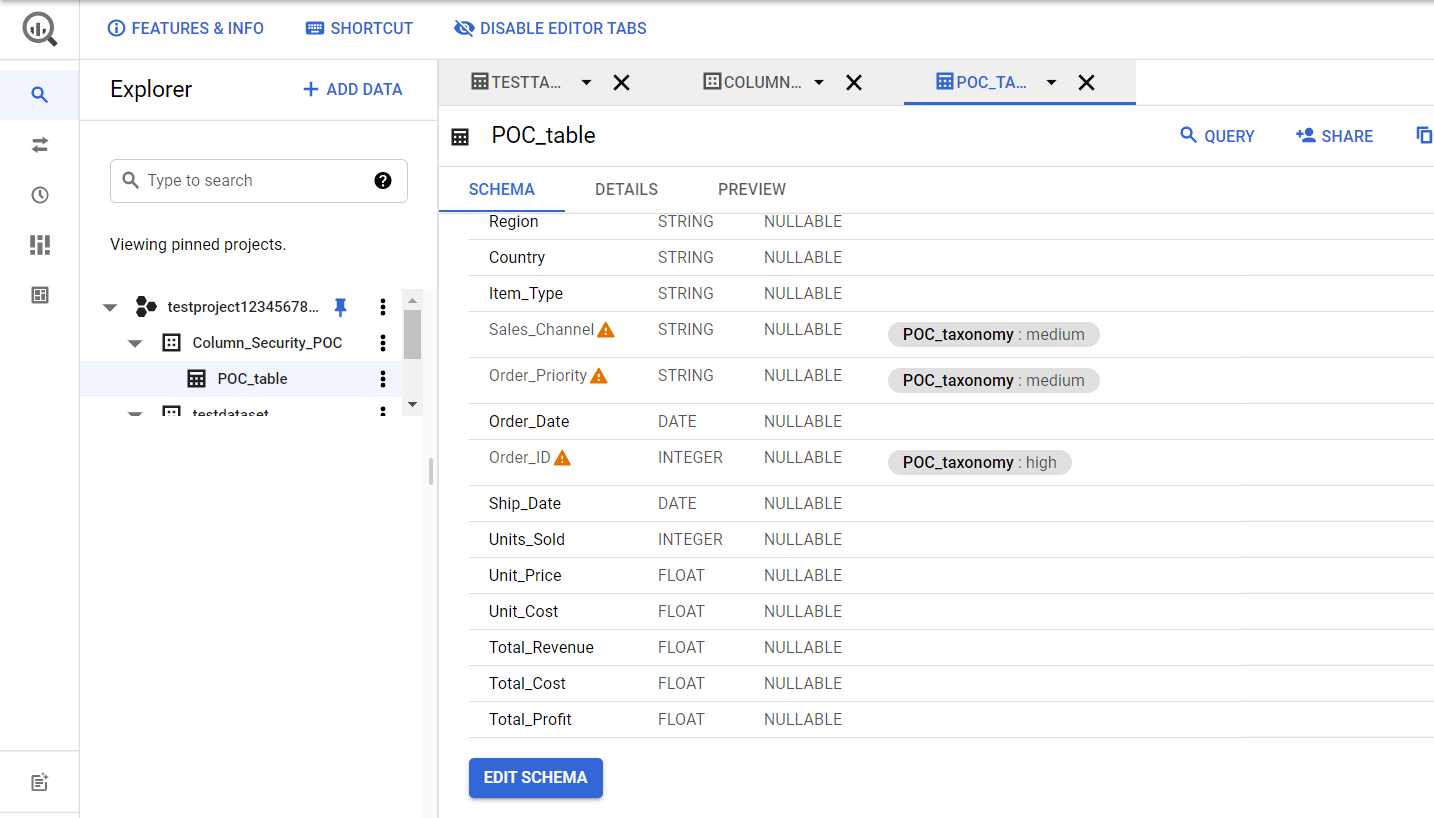




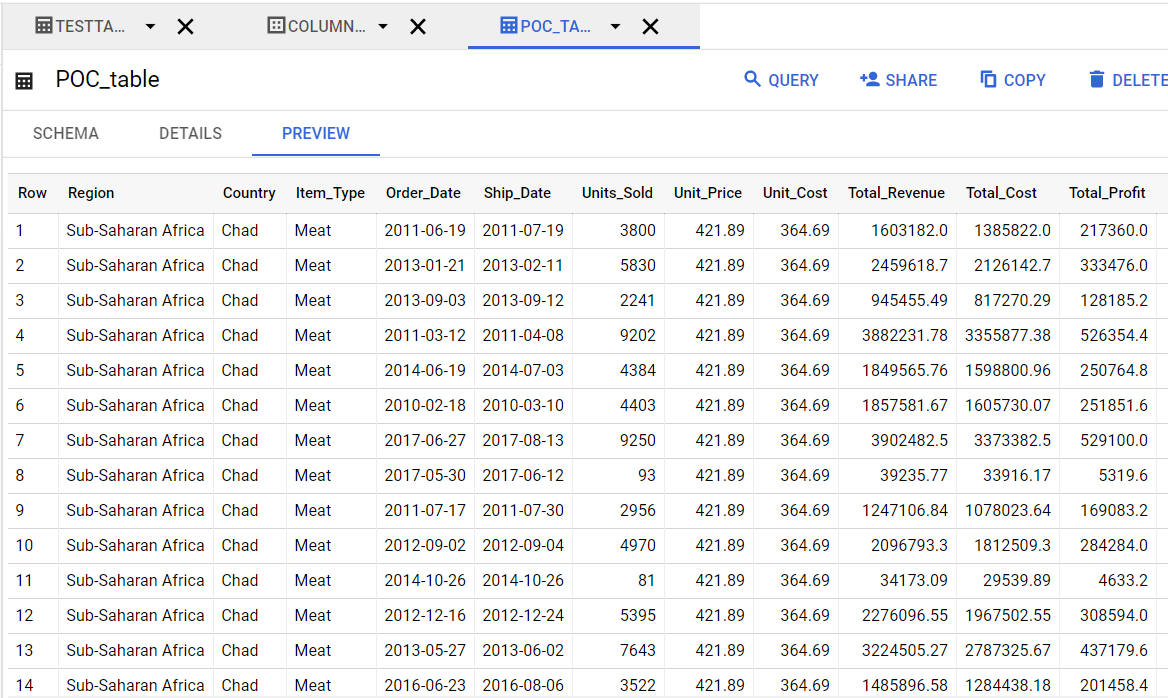
Click on Save

You should see something like this, keep in mind that to add policy tags to column the user needs Policy Tag Admin role.

Data Catalog permissions are implemented along with BigQuery dataset permissions

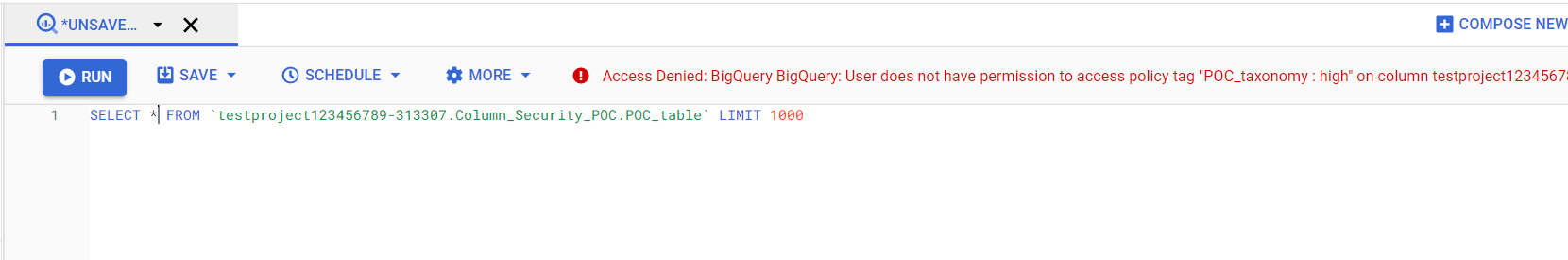


When you click on PREVIEW, the restricted columns won’t be visible

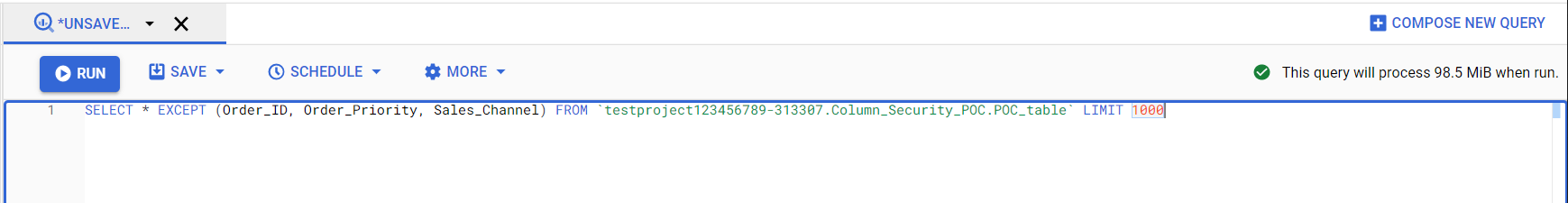


This will enable column-level security to the table and only members with Fine-Grained Reader permission at the resource level of policy tags will have access to view or query the restricted columns

If you try to run queries that include the restricted columns, the query won’t be executed

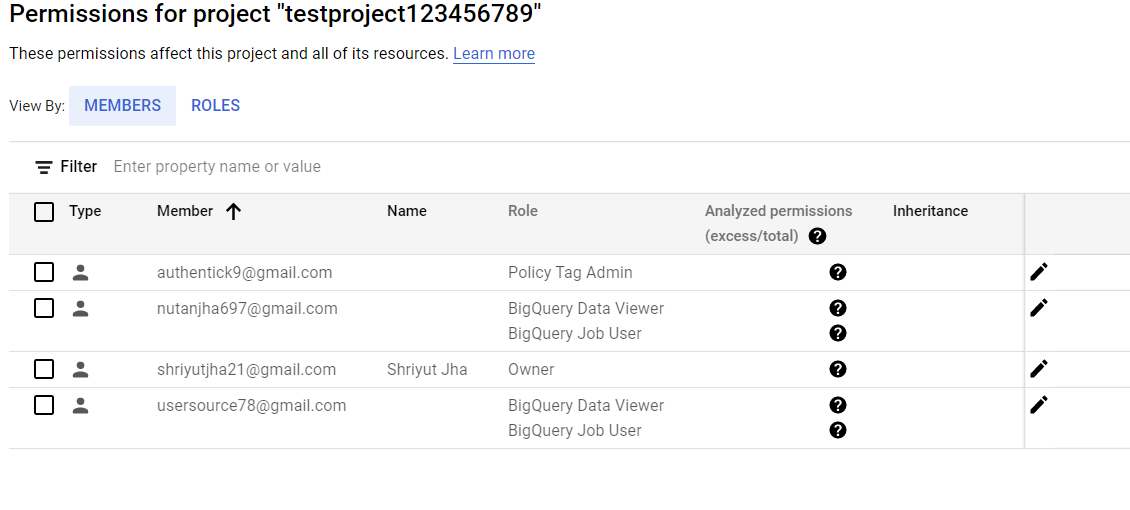


If you don’t query the restricted columns, you won’t receive the error



For this POC we implemented multiple policy tags with different columns, for users to be able to query the restricted columns they need data catalog fine-grained reader role at resource level.

We need to ensure that the user has BigQuery Data Viewer & BigQuery Job User role in IAM.



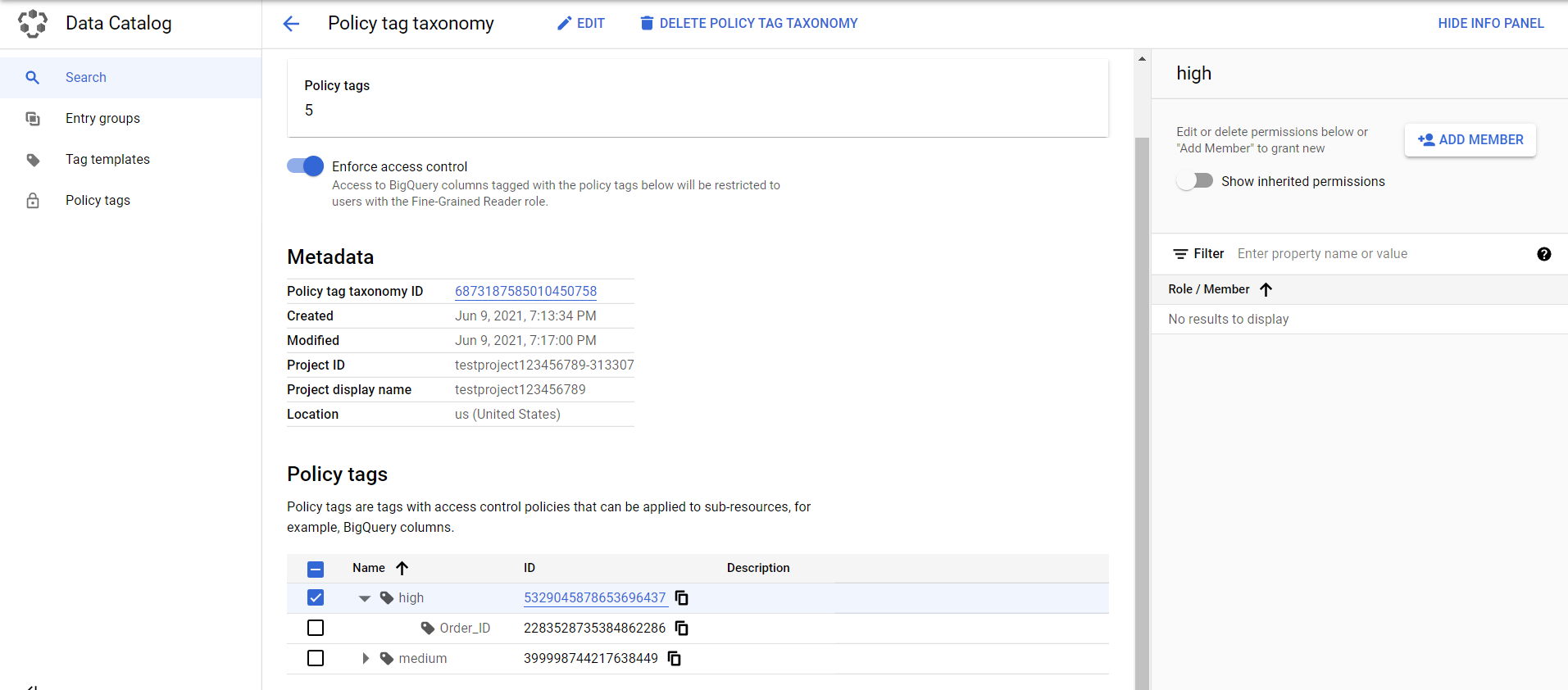
To add permissions for the user

Step-1: Go back to Data Catalog page and select policy tags

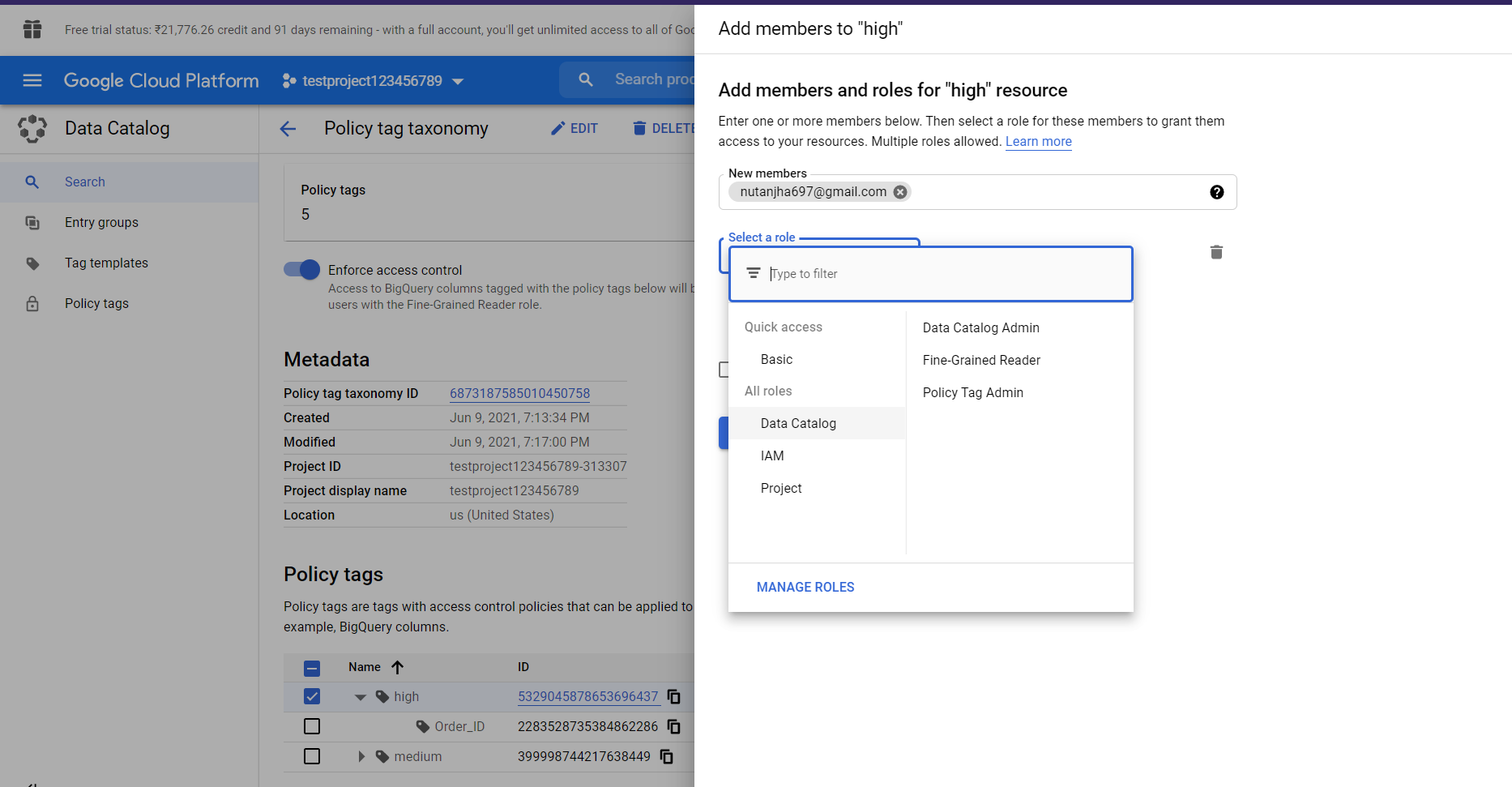
Step-2: Select the taxonomy and click on the policy tags for which you need to add user

Click on Add member

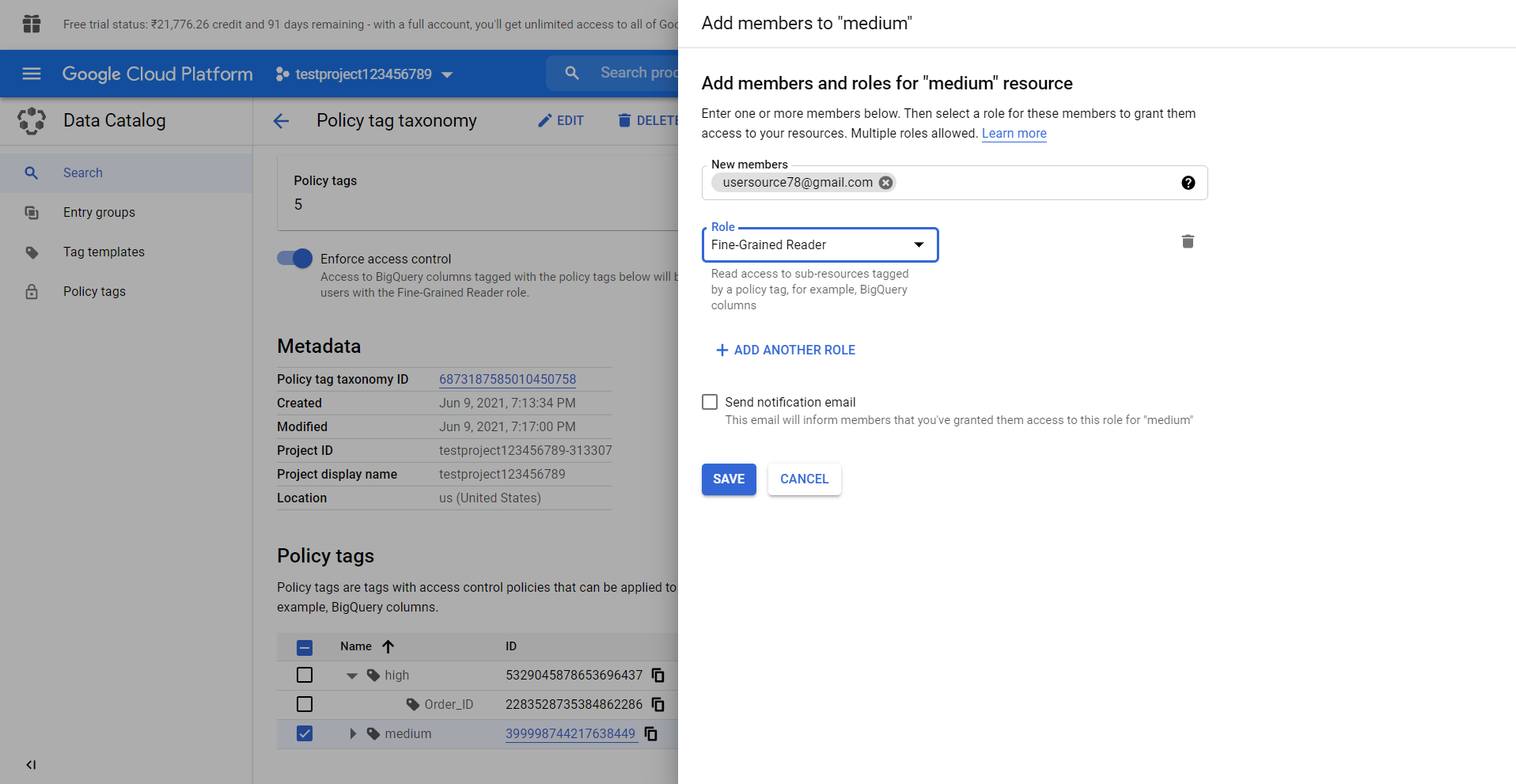
Select the Policy tag from the taxonomy page & Click on Add member



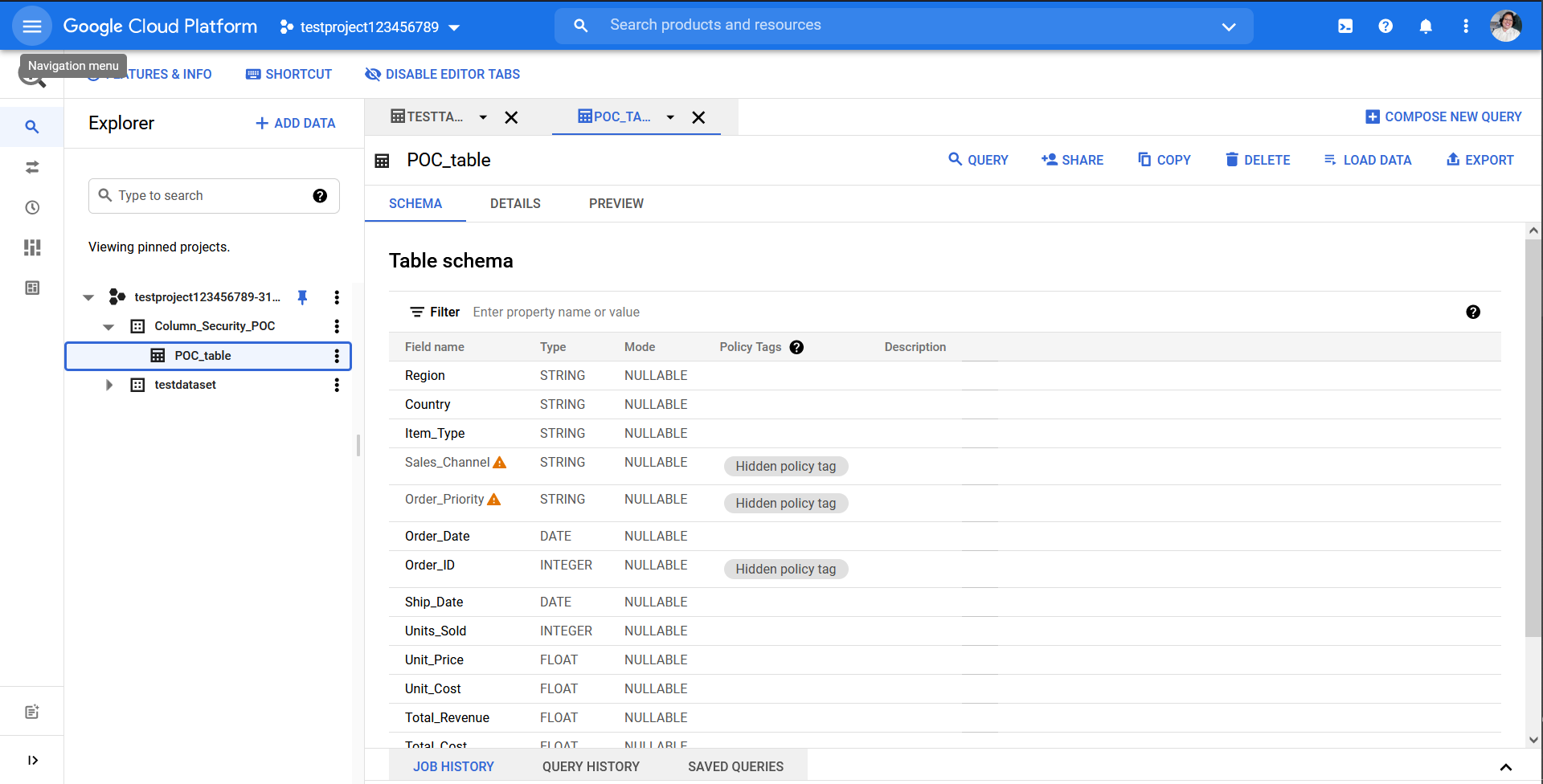
Provide the email address of user and grant them Fine-Grained Reader permission from Data Catalog section



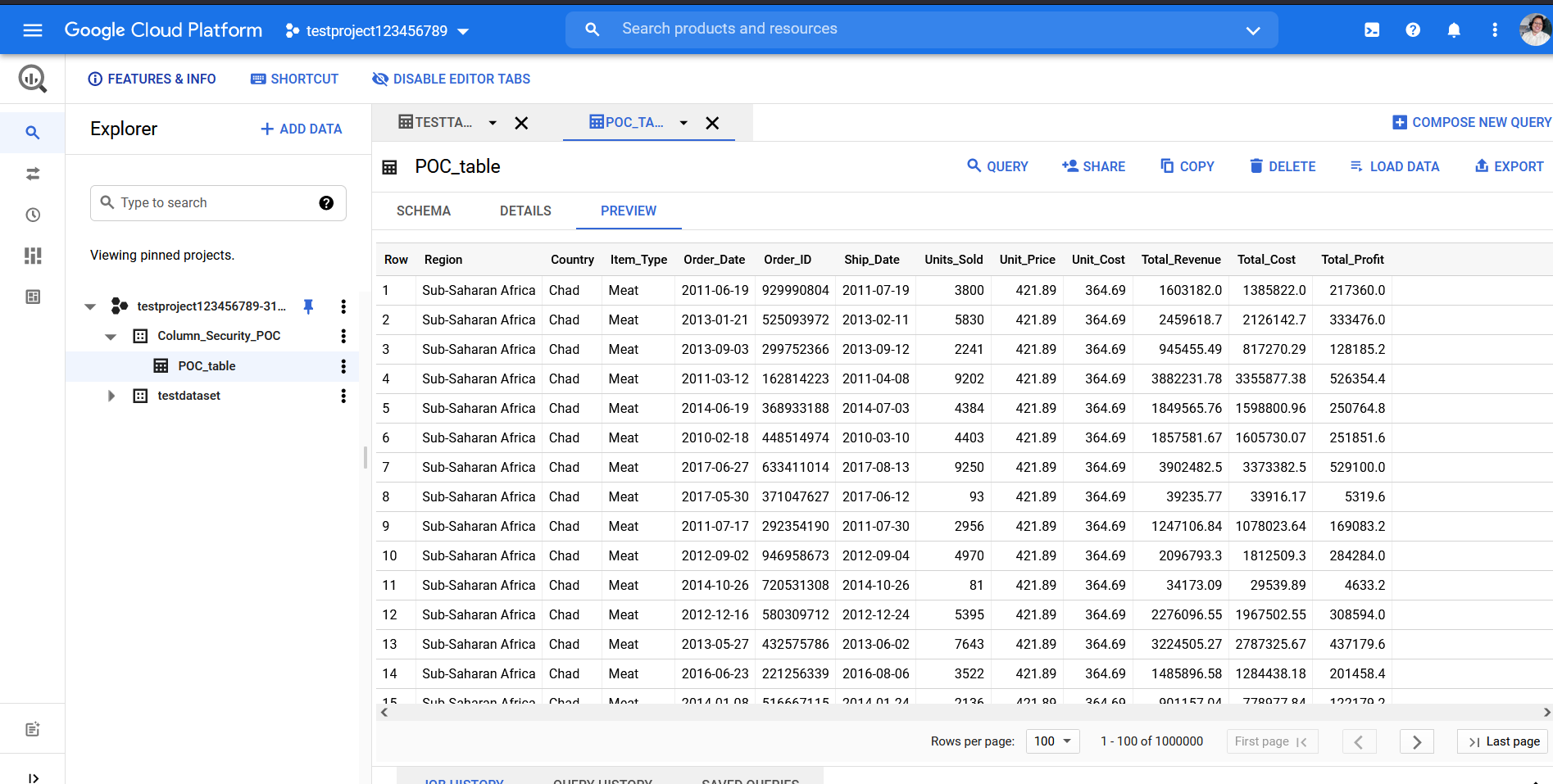
Repeat the same process for other user



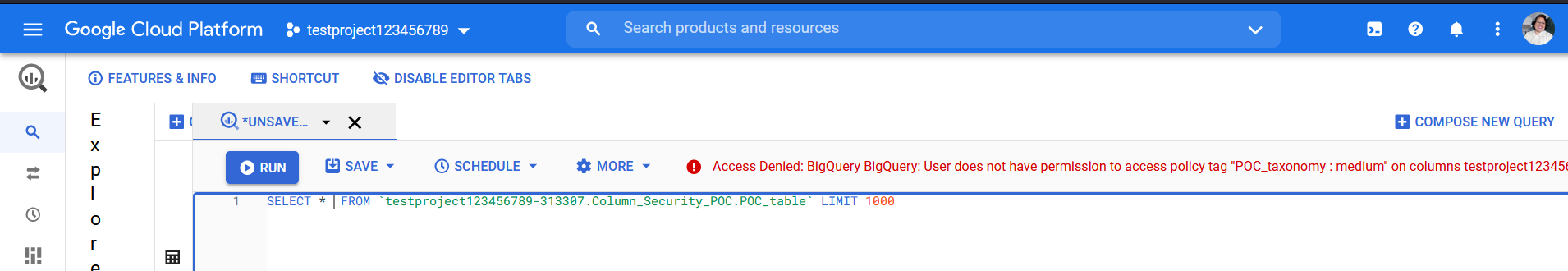
For the user with access to a specific policy tag will be able to view/query columns with that policy tag but not other columns.

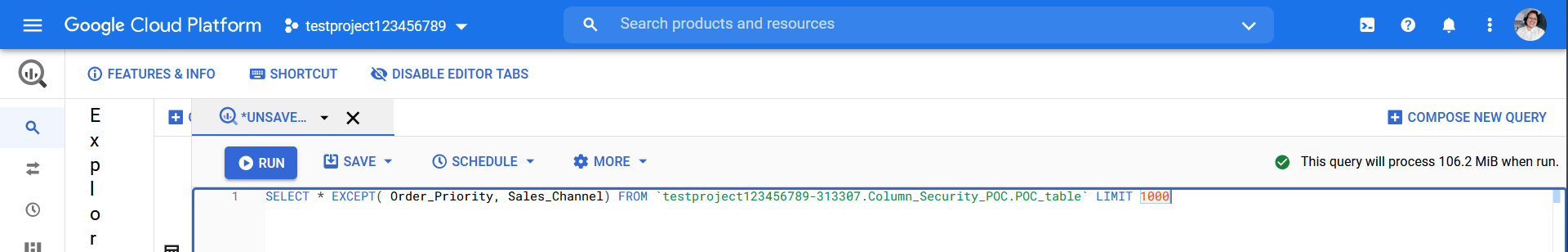


As we can see below Sales\_Channel and Order\_Priority columns are not visible to the user



We get access denied error on running the query on restricted columns





We’re able to run the query on other columns including Order\_ID

Similarly the other user won’t be able to access the column Order\_ID

