This topic shows you how to configure Cloud IAM permissions for a set of sample billing scenarios. It provides guidance on which Cloud IAM roles to grant to the billing-related functional roles in your company for the scenarios. These examples are mainly targeted at billing administrators and employees who manage billing tasks for an organization.

This document does not explain in detail the billing roles and permissions. For a detailed description of roles and permissions for Billing API, read the Access Control for Billing (https://cloud.google.com/billing/v1/how-tos/access-control) page.

In this scenario a small company is trying to configure and use Google billing accounts. They have a handful of engineers who develop and maintain their applications, but none of them manage their billing. They have an office manager, who is responsible for matching payments to invoices, but for compliance reasons the office manager is not permitted to have access to the Cloud Platform resources in the projects. The CEO also holds and manages the credit card details.

The table below explains the billing Cloud IAM roles that the Organization Administrator (which is the CEO in this scenario) can grant to the other personas in the company, and the resource level at which she grants the roles.

Role:	Organization Administrator	The Organization Administrator role gives the CEO the ability to assign permissions to the Office Manager.
Resource:	Organization	
Member:	CEO	

Role:	Billing Account Administrator	The Billing Account Administrator role allows the office manager and the CEO to manage payments and invoices without granting them the permission to view the project contents.
Resource:	Organization	
Members:	Office Manager, CEO	

The Cloud IAM policy attached to the organization resource for this scenario will look similar to the following:

The JSON for all Cloud IAM policy snippets is shown for each scenario. These bindings can also be set via the Cloud
le.

The best practice is to use groups to manage members. In the example above, for the second binding, you would add the CEO and office manager to the `finance-admins-group`. When you need to modify who is able to carry out the function, you simply need to adjust the group membership, negating the need to update the policy. So the two individual user accounts do not appear in the members list.

In this scenario, a large organization wants the finance team in each division to be able to set budgets and view team spending in the division, but not have access to the Google Cloud resources. They don't mind if the developers see the spend for their own projects, but a broad view of expenses should not be allowed to the developers.

Grant the roles in table below to the finance manager of each division and the developers:

Role:	Billing Account Administrator	This role grants the finance manager of each division the permission to set budgets and view the spending for the billing accounts in their divisions, but does not give them permissions to view the project contents.
Resource:	Billing Account	

Members:	Finance manager of each division	
Role:	Viewer	The Viewer role allows the developers to view the expenses for the projects they own.
Resource:	Project	
Members:	Developers of the project.	

For this scenario you will need two separate actions to assign the appropriate permissions Cloud IAM policies as they are attached at different levels of the hierarchy.

Assigning permissions to the billing account:

Use the billing console to grant a user the Billing Account Administrator role on the billing account. From the account that has set up the billing account, grant the finance manager the Billing Account Administrator role on the billing account.

The Cloud IAM policy which needs attaching to the project will look similar to the following:

In this scenario, a customer's central IT team provides Google Cloud resources to their developers as part of their self service portal. Developers request access to Google Cloud projects and other approved cloud services via the portal. The cost center of the developer pays the central IT team for the cloud resources consumed.

The central IT team must be able to:

- Associate projects with billing accounts.
- Turn off billing for projects.
- View the credit card information.

They must not have permissions to view the project contents.

Developers should be able to view the actual costs of the Google Cloud resources being consumed, but shouldn't be able to turn billing off, associate billing with projects, and view the credit card information.

Role:	Billing Account Administrator	The Billing Account Administrator role grants the IT department the permissions to associate projects with billing accounts, turn off billing for the projects, and view the credit card information for the accounts that they resell to their customers. It does not give them permissions to view the contents of the projects.
Resource:	Billing Account	
Member:	IT department	

Role:	Billing Account User	The Billing Account User role gives the service account the permissions to enable billing (associate projects with the organization's billing account for all projects in the organization) and thereby permit the service account to enable APIs that require billing to be enabled.
Resource:	Organization	
Member:	Service account that is used for automating project creation.	

Role:	Viewer	The Viewer role allows the developers to view the expenses for the projects they own.
Resource:	Project	
Members:	Developers of the project.	

For this scenario you will need two separate operations to assign the appropriate Cloud IAM policies as they are attached at different levels of the hierarchy.

Use the billing console to grant a user the Billing Account Administrator role on the billing account. From the account that has set up the billing account, grant the finance manager the Billing Account Administrator role on the billing account.

You then need two separate Cloud IAM policies as you are attaching them at separate levels of the hierarchy.

The first Cloud IAM policy that needs to be attached at the organization level is to grant the service account the Billing Account User role. It will look similar to the following.

The second Cloud IAM policy needs to be attached at the project level. Grant the developers the Viewer role on the project:

A large digital native wants to allow all their developers to create billed projects on their organization's invoiced account without giving them Billing Account Administrator rights.

A project needs to have billing enabled to ensure that APIs beyond the default can be enabled. Thus if a developer creates a project, they need to associate it with a billing account to enable the APIs.

Role:	Billing Account Creator	The billing creator role will enable the developers to: • Create new billing accounts • Attach the billing accounts to the projects
Resource:	Project	

Members:	Developers

The Cloud IAM policy for this scenario needs to be attached at the project level, and it will look similar to the following:

In this scenario, a company wants to calculate and keep track of how much each team, department, service, or project is costing them. For example, keep track of how much does a test deployment cost them each month.

This can be tracked by using the following practices:

- Use projects to organize resources. Cost is shown per project and project IDs are included in billing export.
- Annotate projects with labels that represent additional grouping information. For example, `environment=test`. Labels are included in billing export to allow you to slice and dice further. However, labels on a project are permissioned the same way as the rest of the project's metadata which means a project owner can change labels. You can educate your employees about what not to change and then monitor (through audit logs), or grant them only granular permissions so they can't change project metadata.

You can export to JSON and CSV, but exporting directly to BigQuery is the solution we recommend. This is easily configurable from the billing export section of the billing console.

If each cost center must pay a separate invoice or pay in a separate currency for some workloads, then a separate billing account for each cost center is required. However this approach would require an affiliate agreement signed for each billing account.