Disable Automatic IAM Grants for Default Service Accounts

Disable Automatic IAM Grants for Default Service Accounts

Google Definition

This boolean constraint, when enforced, prevents the default App Engine and Compute Engine service accounts that are created in your projects from being automatically granted any IAM role on the project when the accounts are created.

By default, these service accounts automatically receive the Editor role when they are created.

Affected resources:

- Auto-created Service Accounts

In Solvay...

Auto-created Service accounts by Google services are not to be granted with high administrative priviledges.
This is to avoid these service accounts are used for unintended purposes which will result in audit issues.

All intention of the service accounts must be clearly declared during the building phase.

Service accounts will not be granted with high administrative priviledges (example Owner, Editor).

You need to find out what is really required instead of granting everything.
You are not supposed to use auto-created service account for GCP services (example app engine, compute engine, cloud function) for external usage.
If you need to use by external clients, a user managed service account has to be created with a minimum permission granted.