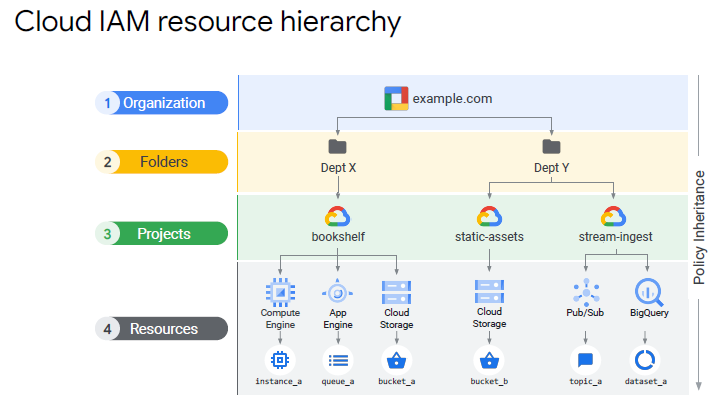
**Essential Google Cloud Infrastructure: Core Services**

**Cloud IAM**

* Identity and Access Management
* Who can do what on which resource
  + Who – person, group or application
  + What – specific privileges or actions
  + Resource – any GC service



Policy

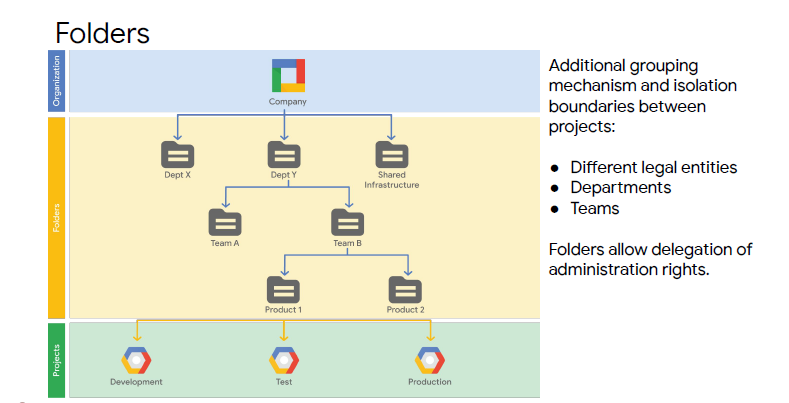
* collection of access statements attached to a resource.
* Each policy contains a set of role and role members, resources inherit policies from their parents.
* Less restrictive parent policy overrises a more restrictive resource policy.
* Child policy cannot restrict access granted at the parent level (if you have editor role at dept X and viewer role at bookshelf project, you still have editor access to bookshelf project)
* Policy of least privilege – select the smallest scope necessary for task to reduce risk exposure.

IAM conditions

* Define and enforce conditional attribute
* Grant resource access to identities if configured conditions are met
* E.g. temporary access in the event of production being down

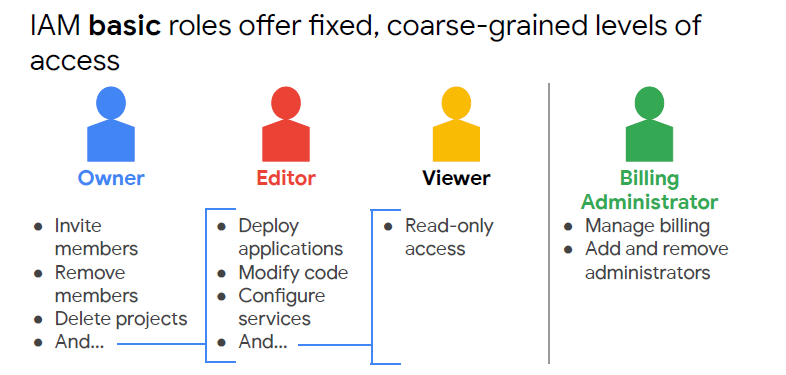
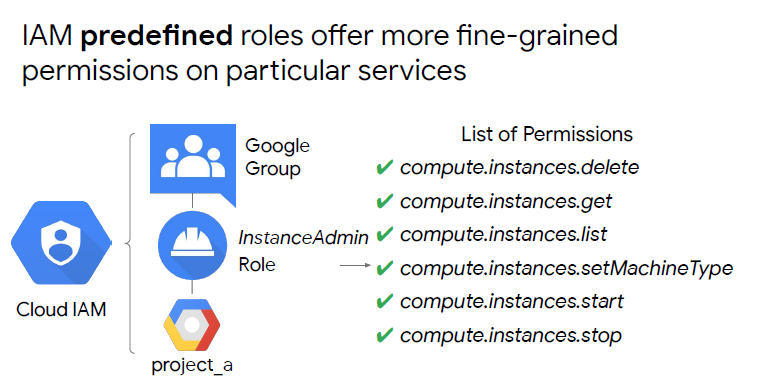
Organisation node

* Root node inf GCP resources
* Organisation Role – control over all cloud resources (useful for auditing)
* Project creator – project creation and control over who can create projects



^Folders can be considered as suborganisations within the organisation

IAM roles

* Basic roles – applied to project and affect all resources in that project (owner, editor, viewer) 
* Predefined roles – defined where the predefined roles can be applied. Provides granular access to specific resources and prevents unwanted access to other resources. Have a collection of permissions
* Custom roles – can define a precise set of permissions