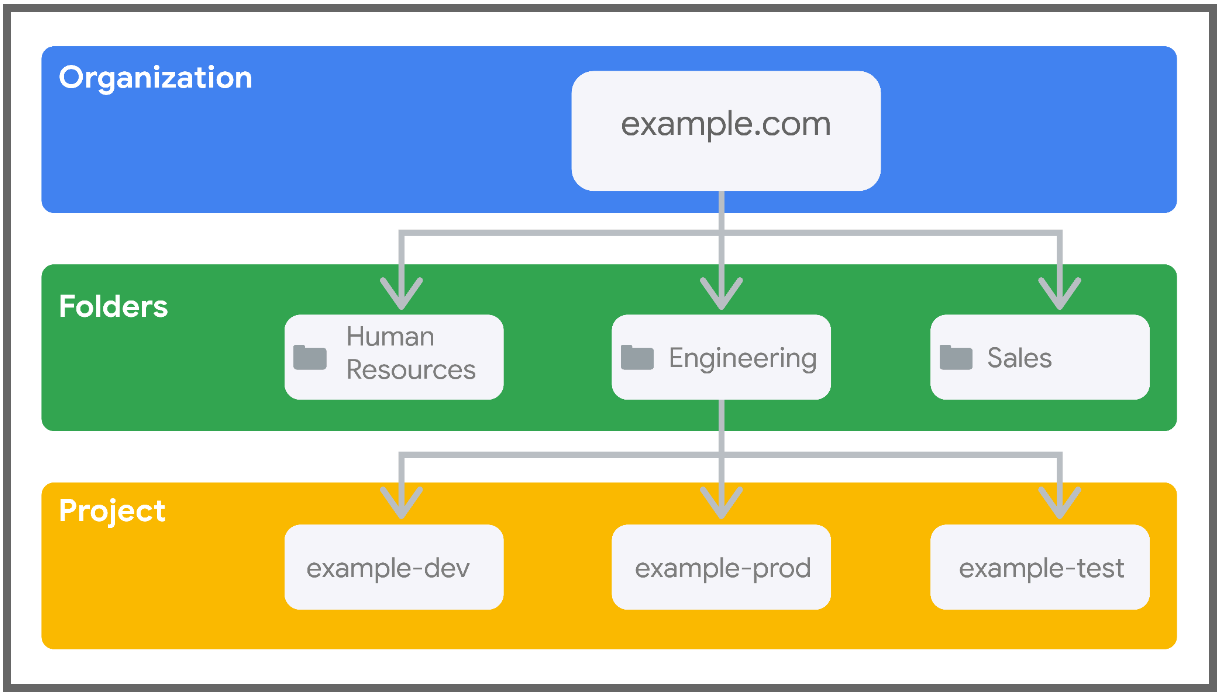
Best practices for Google Cloud resource hierarchy

So far, you've learned that control inheritance is the process of using controls that are already provided by a cloud service provider. You've also examined how hierarchies in the cloud help engineers learn how the parts of their organization are arranged inside of the cloud environment. Hierarchies also enable the security team to put policies and controls into place within an organization. In this reading, you'll learn more about the Google resource hierarchy. You'll also review some best practices for using Google resource hierarchy for access control.

Google Cloud resource hierarchy

The purpose of the Google Cloud resource hierarchy is to provide a hierarchy of ownership. Ownership binds a resource to its immediate parent in the hierarchy, and provides inheritance for access control and organization policies.

The Google Cloud resource hierarchy resembles the file system found in traditional operating systems. It works by organizing and managing entities from the top, and cascading down. This hierarchical organization of resources enables you to set access control policies and configuration settings on higher level resources. The policies and Identity and Access Management (IAM) settings are then inherited by the lower level resources.



Best practices for Google Cloud resource hierarchy

- Your Google Cloud resource hierarchy must mirror the access control model. For example, accounting may not need a separate folder or project, but development and ops may need one or more folders.
- Use projects to group resources that share the same trust boundary. A trust boundary is where two principals, like people and services, are interacting with data. For example, an interaction might be to pass data or to issue an instruction about data. The trust boundary is the point where an authentication and authorization have to occur to allow the action. For example, resources for the same product or service can belong to the same project.
- Grant roles to a Google group instead of to individual users when possible. For more information about how to manage Google groups, see Google Groups help.
- Use the security principle of least privilege to grant IAM roles. This means, only give the least amount of access necessary to ensure that workflows remain operational.
- Grant roles at the smallest scope needed. For example, if a user only needs access to publish messages on a specific topic, only grant the publisher role to the user for that topic.
- If you need to grant a role to a user or group that spans across multiple projects in the same folder, set that role at the folder level instead of setting it at the project level.
- Use labels to annotate, group, and filter resources. Labels can help you organize resources. You can attach a label to each resource, then filter the resources based on their labels. For example, you could use labels to group virtual machines in categories like production, staging, or development so that you can search for resources that belong to each development stage. After adding labels to your resources, you can take advantage of the nested filtering feature to perform more precise searches for your labeled resources.
- Audit your allow policies to ensure compliance. Allow policies are also known as Identity and Access Management (IAM) policies, which are attached to resources. You can attach only one allow policy to each resource. The allow policy controls access to the resource itself, along with any descendants of that resource that inherit the allow policy. This means that users don't have access to a resource by default. Users have to be granted explicit permission to the resource to use it.
- Audit the ownership and the membership of the Google groups used in allow policies.

Pro tip: Each cloud provider publishes resources highlighting security best practices. Take the time to read and follow their recommendations for structuring resource hierarchies. This will help you better understand the types of security controls you can implement at each level, based on the data you're processing.

Key takeaways

Hierarchies help enable security teams to put policies and controls into place within an organization. The Google Cloud resource hierarchy provides inheritance for access control and organization policies. Knowing about the best practices for setting up and maintaining a resource hierarchy that meets your organizational and compliance needs is an important part of cloud security.

Resources for more information

Check out these resources to learn more about Google Cloud resource hierarchy:

- Google cloud security best practices center
- Learn more about organizing resources using labels.
- Learn more about understanding allow policies.