Higher Ed GCP Adoption Guide

NOTE: This document is the byproduct of the work of several schools involved in the Internet2 NET+ Program and its service advisory board. If you choose to use any of this content elsewhere, please give credit where credit is due.

Before the Contract

Preparation Steps

Your Existing Google Footprint

These details are high level but will be useful when you begin discussions about GCP internally and with external consultants. If you do not currently have a GCP/G Suite domain, your answers can reflect your desired state.

Identity

Identity management questions seek to determine how your user accounts are currently managed. There are several options for account management in Google, including syncing from local systems, using G Suite identities, or using Google Cloud Identity.

Target Audience and Roadmap

These details will help you get started with planning the organizational structure, security requirements, roles and responsibilities, support, and implementation priorities.

Assembling your Implementation Team

The answers to these questions will help you during your contracting, implementing, and operations phases of your GCP service. There are no wrong answers! And you don’t have to

answer all questions before you start, but it will be useful to refer back to this table as you go forward.

Your Google Footprint	Example answers, to help you on your journey
Does your institution have any G Suite domains? List them:	example.edu, example2.org, example.com, subdomain.example.edu
How is G Suite made available to your institution?	Only Drive is available via the example2.org domain.
Is GCP available to your institution? Describe	GCP is turned on but limited to active accounts in example.edu.
How many projects exist in GCP already (if applicable)?	
How many billing accounts exist in GCP (if applicable)?	
Are/Will default networks be used?	
Do you already have dedicated private IP addressing space reserved for GCP? What subnets and what are the associated CIDRs?	
Identity Management	
What is your institution's IAM system?	On-prem Active Directory
How does your institution manage identities in Google G Suite?	Synchronized from Active Directory via Google Cloud Directory Sync
How often do users sync?	Four times a day, roughly every 6 hours.
Do you sync passwords?	No, not currently.
How do users authenticate?	SSO
Does your institution use Google Cloud Identity?	
Target Audience and Roadmap	
Who will have access to GCP? (Faculty, Staff, Students, other..)	*All will have access, but only certain populations will be able to create projects.*
What are the intended use cases in GCP?	

(Research, Teaching and Learning, Administrative Systems)	
Does your institution intend to allow any 'sensitive data' types into GCP? (Data subject to FERPA, PHI, HIPAA, GDPR, DFAR 252.204-7012, etc.)	Yes, HIPAA and FERPA data will be in GCP
Do you already have an anticipated annual spend?	
Are there any other specific and immediate needs related to GCP that are motivating your work?	
How will resources be provisioned in GCP? Deployment Manager or Terraform, or other?	
How will users get access to Galok and support?	
Will there be centralized or departmental invoicing?	
Does your IT organization have an existing SIEM that will be used to collect GCP logs?	
Implementation Team	
***Who is making executive decisions about the implementation**? Who owns the service? Who will support the service after implementation?*	
***Networking expert:** This person should understand your institution's network, and the implications of a new public cloud service on your network architecture, including a Google Interconnect or VPNs.*	
***Identity Management:** This person should understand how IAM is managed at your institution, and will be useful during discussions about user account management, Google Groups, and access for external collaborators.*	
***Security:** This person should be able to clearly define your institution's technical requirements for public cloud resources, and also able to establish requirements for logging and monitoring of cloud resources (from a security perspective).*	
***Compliance/Legal:** This person should be able to*	

describe the implementation requirements related to the types of data/usage anticipated in GCP.	
Billing and Procurement: *This person should understand your institution's procurement practices and, importantly, preferences for ordering and invoicing cloud services. Ultimately, one bill for the institution that is distributed internally, or multiple POs and invoices distributed per project/billing ID.*	
Google G Suite Admins*: If G Suite and GCP are managed by separate teams, a G Suite Super Admin should be included. Assists with implications of Google Groups, IAM, and can assign roles in GCP.*	
Cloud Architect*: If available, this person will assist with making decisions related to policy, folder structure, and other configurations, and will be part of implementing the actual solutions.*	
(Optional) Administrative Systems Developers*: If you are implementing GCP for administrative systems, you should include appropriate team members to assist with decision making.*	
(Optional) ITSM Developers, DevOps team members, etc.	
(Optional) Communications *How will you communicate the offering(s) and decision(s) about GCP to your stakeholders?*	

GCP Basics

Identity - G-Suite and Cloud IAM

G-Suite provides identity for the entire Organization and various Google products. Cloud Identity and Access management is a service of Google Cloud platform that can be used with G-suite or independently. It is used to control access for Org node, folders and projects. It governs what level of access users in a project have to manage other services and resources.

Google Groups

Google groups are how Cloud IAM is applied to a collection of users. Groups are used to grant and change access controls for a whole group at once instead of granting or changing access controls one-at-a-time for individual users or service accounts.

Permissions

Permissions determine what operations are allowed on a resource. Each service in GCP has a set of predefined permissions and access to each service is governed by a set of permissions called a ‘role’.

Role

A role is a collection of permissions. You cannot assign permissions directly to users; instead you grant the user a role. When you grant a role, you grant all the permissions that the role includes. There are three types of roles in GCP.

Primitive Roles

These are the Owner, Editor, and Viewer roles. These are legacy roles that represent broad sets of permissions.

Predefined Roles

Predefined roles give finer-grained access control than the primitive roles. They are designed for specific services and the tasks one might need to do with the service. For example, the predefined role Pub/Sub Publisher (roles/pubsub.publisher) provides access to only publish messages to a Cloud Pub/Sub topic.

Curated roles

Roles created by combining two or more predefined roles

Custom roles

Roles that you curate to tailor permissions to the needs of a use case when predefined roles don't meet your needs. This can be a set of permissions or a collection of predefined roles bundled into a new role. While custom roles give the greatest granularity of control, they require the most maintenance and their underlying permissions are subject to change without notice.

Comparing GCP to AWS and Azure

Competitive Comparison

https://www.datamation.com/cloud-computing/aws-vs-azure-vs-google-cloud-comparison.html

Terminology

Technical

	GCP	AWS	Azure
Compute	Compute Instances	EC2 Instances	Azure Virtual Machines
Storage	Cloud Storage, Persistent Disks	S3, Glacier	Storage Accounts, Blob Storage, Disk Storage
Network	VPC	VPC	VNET
Database	Cloud SQL	Aurora, DynamoDB, RDS	Azure SQL, Cosmos DB, SQL Server on Virtual Machines
Container Orchestration	Google Kubernetes Engine (GKE)	Elastic Kubernetes Service (EKS)	Azure Kubernetes Service (AKS.)
App Hosting	Cloud Functions	Cloud Functions	Functions, Logic Apps
Common VDC Boundary	GCP Project	AWS Account	Azure Subscription

Management

	GCP	AWS	Azure
Enterprise Environment	Organization	Organization	Enrollment
Organizational Container	Folders	Organizational Units	Management Groups
Customer Environment	Projects	Accounts	Subscriptions
Services	Resources	Resources	Resources
Resource Factory	Deployment Manager	CloudFormation Templates	Azure Resource Manager + Blueprints
Policy Container	Folders	Organizational Units	Management Groups
Policy Mechanism	Organizational Policies	Service Control Policies	Policies

Project Segmentation	(Tagging)	Tagging	Resource Groups
Default Billing Endpoint	Billing ID	Account	Enrollment

Substantive Implementation Differences

Account Structure

IAM

For most Higher Education customers, GCP identity is tied to G Suite / Google Workspace.

Billing

Whereas in AWS and Azure, the account (or subscription) itself is the billing endpoint, in GCP a project is only associated with a billing endpoint (billing ID). This can be a many-to-one relationship and the billing IDs can be swapped out.

How billing works in GCP

Billing Account/ Billing ID

A Billing Account is the payment source associated with GCP projects to which costs are charged. No work can take place in a GCP project without a valid Billing ID. A Billing ID serves as a user's GCP "line of credit" for their work in GCP. Multiple projects can be linked to a single Billing ID. Billing ID's are generated in one of the following ways:

Self-Serve

A Billing ID is generated when a user sets up an account with their credit card details.

Contracted

Billing ID generated by the reseller at the request of the campus cloud team with a valid purchase order.

Credits

Teaching Credits

Faculty request credits for themselves and their students. They usually come in $50 increments. These credits can be entered at a special URL that will generate

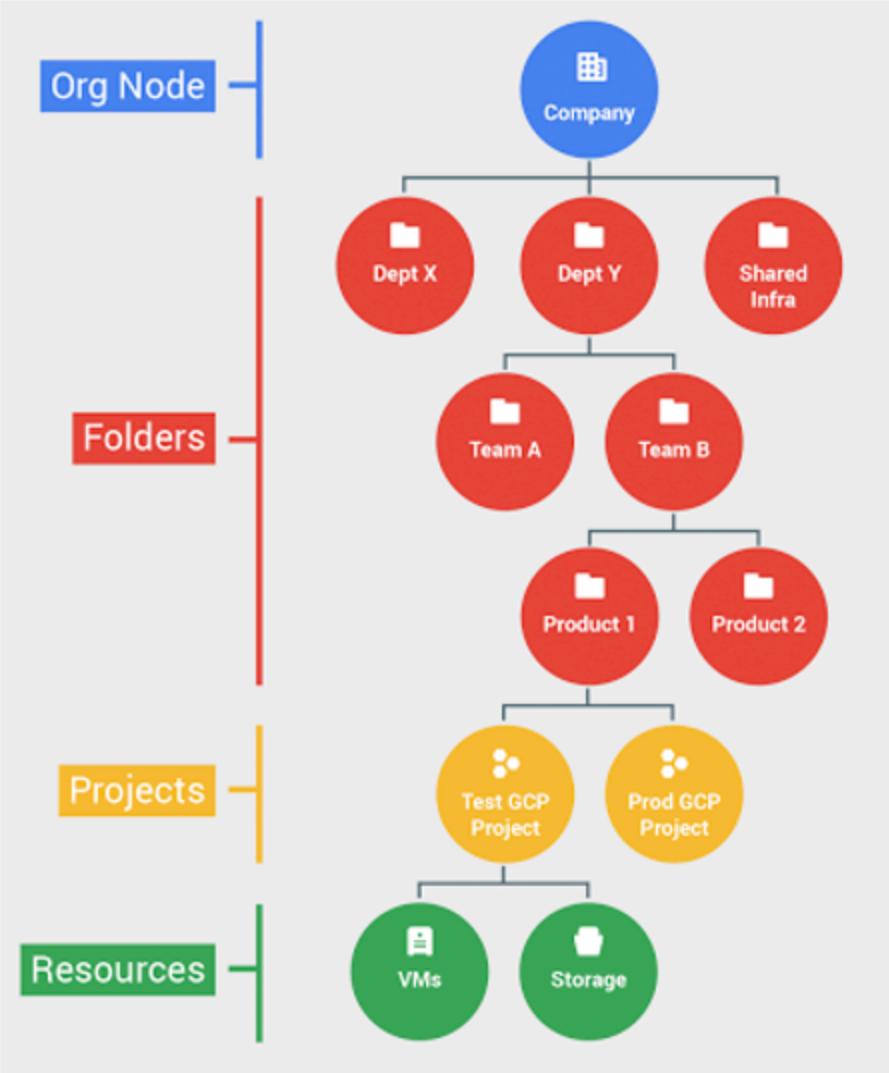
Billing IDs without requiring credit card information.

Research Credits

Google offers researchers up to a $5000 computing credit to experiment with GCP. These can only be applied to an existing Billing ID. Unlike teaching credits, they do not generate their own Billing ID and must be established through the contracted process. Researchers may apply for larger grants through a proposal process.

GCP organizational structure

- A GCP **Organization** is currently tied to a G Suite or Google Cloud Identity Domain. There are pros and cons to that arrangement and Google is currently working to address the concerns raised by the tight link.
    - Whether or not your institution already has a test G Suite organization, you should set up a test GCP organization as a sandbox for creating folder structures, testing policies and automations.
        - NOTE: A test Org is not a substitute for good dev/test/prod practices in your production Organization.
- A **Folder** is both an organizational and a security concept. They are used to separate projects into logical groupings and to apply policies and permission at the appropriate levels.
    - NOTE: GCP is currently limited to ten folder levels.
- Projects are the conceptual containers or workspaces. It is the rough equivalent of a Subscription in Azure or an Account in AWS.
- Resources are the tools and services one leverages to accomplish your objectives



Security and Policy

Networking

Contract Decisions

NET+ or Direct?

NET+ Contract

Basics

- Internet2 NET+ program standard program

Program Benefits

- Terms pre-negotiated by a NET+ Service Advisory team, with multiple campuses contributing to the final contract: Indiana University, Michigan State University, University of Washington, and Washington University in St Louis.
- Choice of resellers, with some differentiation (see Reller Profiles); identical terms for all resellers
- Ability to bring your own authorized software reseller to the program, which will add them to the pool of resellers in the GCP in the NET+ Program.
- RFP template available for use in RFP solicitations, to issue competitive RFPs within the NET+ GCP program.
- Discount
- Data Egress Waiver (not exclusive to NET+ program)
    - https://cloud.google.com/billing/docs/how-to/egress-waiver
- Most resellers are STRIDES ready (separate contract, with different terms)
- Program sweetener: [Getting started package]
- BAA (with reseller)
- Service Advisory Board
- Program Benefits (as published by Internet2)

Contractual Call-outs

- FERPA compliance language
- BAA
- Student use is separated for liability purposes
- Higher aggregate liability cap
- Specific liability call-out of breach notification costs, extended to BAA

- STRIDES (NIH)
    - Available only to NIH researchers
    - A separate agreement that sits alongside your NET+ GCP contract. Will be with the same reseller, incorporates the NET+ “Terms of Use”, and has a different (better) discount schedule.

Direct Contract without reseller

Basics

- You negotiate terms and conditions, based on standard GCP public sector contract
- Additionally, you’ll need a separate contract with Carahsoft for NIH STRIDES

Benefits

- Most flexibility to configure the environment to meet your institution’s needs
- Potential to negotiate terms not included in NET+ agreement
- Ability to provision projects and billing accounts right away
- Ability to use billing subaccounts to further customize how resources are billed for
- Data egress waiver available (also in NET+ Program)
    - https://cloud.google.com/billing/docs/how-to/egress-waiver

Onboarding Decisions

Organizational Structure

Folder structure in GCP allows admins to organize projects in order to efficiently enforce policies and rules, assign roles safely, and reduce risks within the environment.

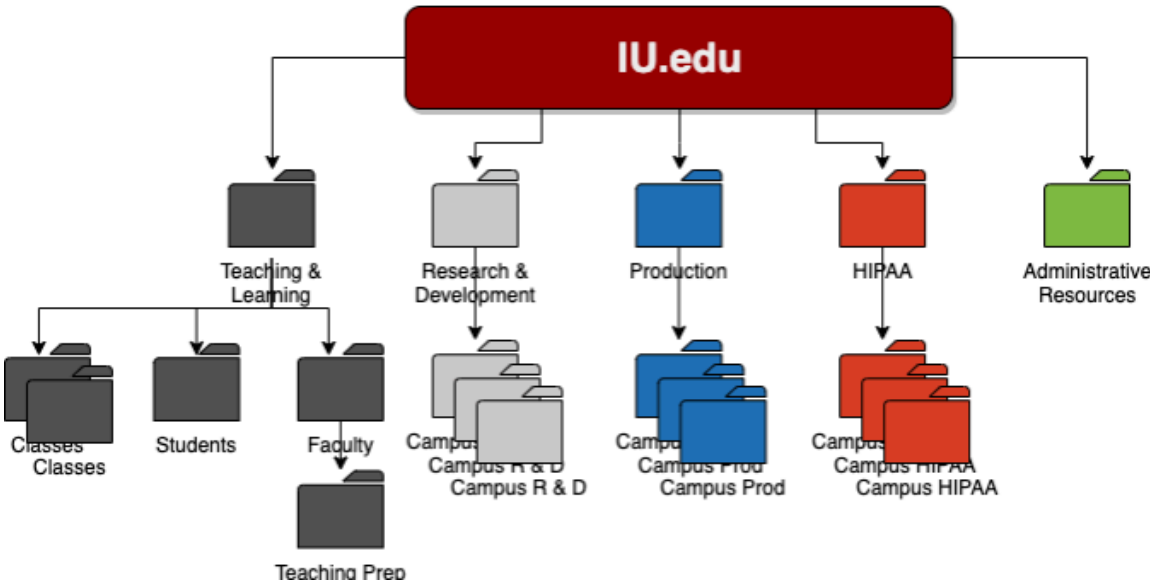
Projects that currently exist outside of the organization can be migrated.

Possible Models

Organizing by Use Case

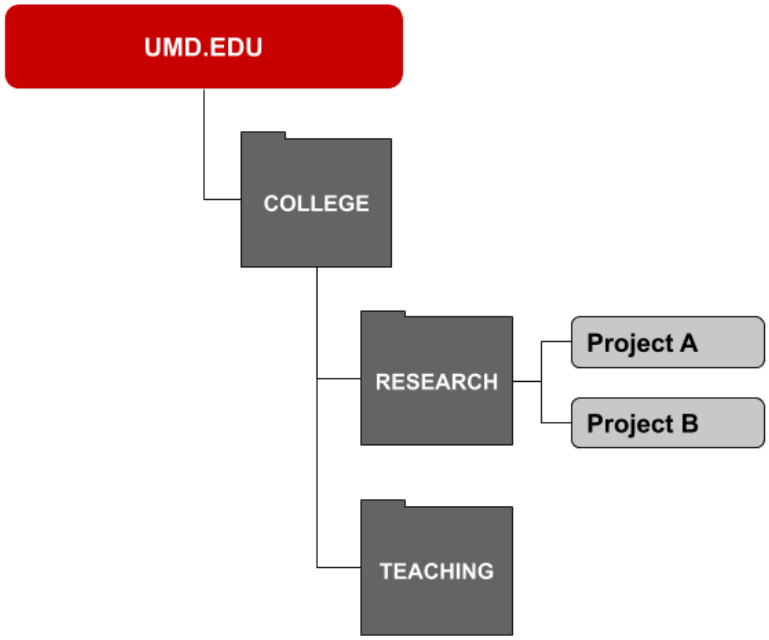
The following structure uses top level folders based on use case categories. Teaching and Learning is separated into Student and Faculty folders because student and faculty accounts

already exist within the GCP domain. Roles are assigned using Google Groups per folder so that, for example, students can create projects in the student folder, but not the other folders. Organizing by use case helps keep policies consistent across projects with similar purposes.



Organizing by College or Department

An alternative organizational approach is to create folders aligned with campus groups, and then create use case folders as the next layer. While GCP admins and central IT can enforce policies, rules, and native roles, decentralized IT support can be granted admin roles for relevant folders. This structure also allows billing and billing roles to be organized by college or department, depending on the need. In this GCP Domain, only Faculty, Staff, and Graduate Students have accounts. Undergraduate students do not have access to GCP by default and their accounts are in a separate Google domain.



- Using Google Groups at the folder level to control roles.
- Create flexibility that allows Billing IDs to be used to their full extent or to be granular when desired.
- In a decentralized environment, create structures that will enable local support in the long run.

Self-Service Project Folder

Security and Monitoring

Cloud Security Command Center

Google Overview of Security Command Center

Security Command Center is a security and risk database with analytics and a dashboard to view vulnerabilities and threats. There are two tiers of Security Command Center: Standard (free) and Premium (min. $25k).

Standard Features

- Detection of public resources
- Web Security Scanner Custom and Scheduled scans

Premium Features

- Event and Container Threat Detection
- Web Security Scanner Managed Scans
- Security Health Analytics: monitoring and reporting for CIS 1.0, PCI, NIST 800-53, ISO 27001

Operations

Are there compliance rules affecting logging?
Are any external log aggregators or SIEMs going to be used? If so, which ones?
What critical metrics and alerts are required for infrastructure?
Is there a log retention requirement? How long? How frequently are these logs accessed?
Should logs be exported to GCS or BQ or both?
Who has access to these logs?
Are there any other governance or compliance requirements to design for?

Forseti

Project Creation

Institutions can choose to remain with the project creation defaults (anyone can create), or tighten controls to only allow permitted users/groups to create projects in an approved folder structure (see example hierarchy diagrams above).

For G Suite institutions, it is very likely that GCP projects already exist in the environment. These could be manually created projects, or auto-created projects from Google AppScript.

Internet2 maintains a github community for GCP member schools to share code at github.internet2.edu. Some members have already shared approaches for gathering information about existing projects.

Project Creation Controls

GCP vs G Suite Admin Ability Comparison	
GCP Admin	**G Suite Admin**

Once the developer console is enabled in Google Workspace, GCP Admin has default permission to create or grant GCP roles.	Controls access to Google Developer/Cloud Console & AppScript Default permission to create or grant GCP roles. Controls access to domain-wide delegation permissions if projects need for G Suite service API

Project Creation Approaches

PROS	CONS
EVERYONE CAN CREATE	
This is the default configuration. No overhead required from GCP Admins to facilitate project creation.	Project sprawl. Valley of forgotten projects. Billing linked to personal credit cards if billing account creation is permitted. Billing not linked to the payments profile named in the Internet2 GCP contract, meaning benefits may not be realized (egress). May not be in-sync with institutional policy regarding expenditures. May cause business continuity issues as people leave the institution, credit cards expire etc.
RESTRICT CREATION	
Control which groups of people can self-create projects still. IE: Allow students to create in a specified “Student Projects” folder, but restrict “Employees” from self-creating. Ensure all projects that incur cost are funneled through the I2 GCP contract,	Additional overhead for GCP Admins depending on level of restriction or self-service options made available.

ensuring visibility and benefits (egress).	

Billing Structure

A Billing ID is typically a unique identifier for a funding source. If permitted, a billing ID can be created by:

- A user when they sign up for a free tier account, backed by their credit card.
- A reseller when they are issued a PO by your institution.
- A user redeeming Google education credits at https://console.cloud.google.com/edu

Note: In certain cases, a reseller may be able to associate multiple funding sources (POs) with a single GCP Billing ID, but this may not be possible with all resellers.

A user/customer can have multiple billing IDs if they have multiple active funding sources and need to maintain separation of costs. Your institution can have

1. A single billing ID and leverage sub-billing IDs to rebill internally
2. At least one billing ID for each customer/project etc.

Note: In a Higher-Education setting, it's difficult to expect any institution to remain with a single Billing ID, mainly because of the way credits (research mainly) are handled. The Single ID Billing approach is undone as soon as the first project with sponsored credits is created.

Institutions can choose to remain with the billing creation defaults (anyone can create), or tighten controls to only allow permitted users/groups to create billing accounts.

In the NET+ context, the billing ID always comes from the reseller. Different billing IDs can have their own contexts, like having the STRIDES discount applied by the reseller. A billing ID can therefore be from an external funding source, like the reseller, the NIH, NSF, or others. This gives the institution the ability to manage a project in its Org regardless of the funding source (e.g., CloudBank).

Quick Reference: GCP / AWS / Azure Billing Comparison

GCP	Billing can be configured on a project-by-project basis, or via single master bill/payment, or variations in between. Billing is not inextricably linked to a project/resource. Billing for projects can be changed as needed.
AWS	Billing is inextricably linked to the account/workspace itself. They are one-to-one and ever linked. While you may change how you pay your bill, it's always tied to one account. A reseller may create consolidated bills for multiple accounts.
Azure	Your Enterprise Enrollment receives a single bill (via your reseller) and you either pay that entire bill or you have your reseller create bills for each "subscription" holder.

Quick Reference: Single vs Multiple Billing ID

TYPE	**PROS**	**CONS**
SINGLE	Faster account provisioning because you don't have to go through the institutional PO creation process. You can hand a user a project and connect it to your main billing ID.	Internal institutional rebilling process must be in place (unless one entity is picking up the entire bill.) Still may need to create separate billing IDs for researchers (needed to apply credits to) or externally funded billing IDs

MULTIPLE	Limited ongoing admin overhead. Once the PO-to-billing ID connection is made, the normal invoicing process runs. Clear cost management for almost all costs. No need to parse credits, egress waivers, marketplace costs etc -- they all go to the Billing ID Some resellers may support linking to a Credit Card (instead of a PO for additional service charge).	Slower account provisioning. (If not using credit cards) The user must create a university PO which goes to the reseller, which then requests the billing ID from Carahsoft, who sends it back to the reseller, who sends it back to the university, who uses it to get the project working for the customer.

Single Billing ID (info moved into table above, but keeping comment until group review says we can resolve it)

An example of why multiple billing IDs is likely to be reality for your campus, is for programs like NIH STRIDES. <need details here>

Support Plan

Operationalizing GCP

Project Creation

Deployment Manager

Terraform

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~Notes~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Reseller feedback:

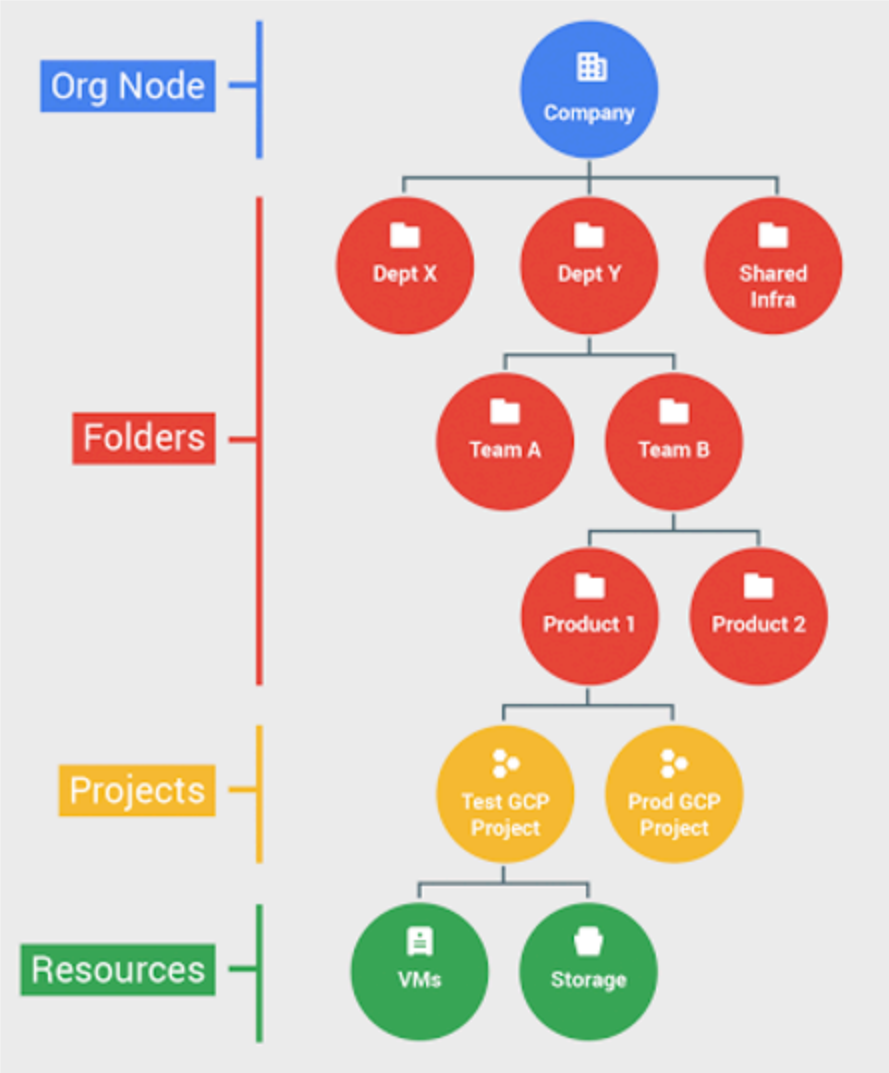
- Be more prescriptive early on
- Nearterm guidelines and what can evolve
- It really needs to be an enterprise service and not a departmental service
-

Possible order:

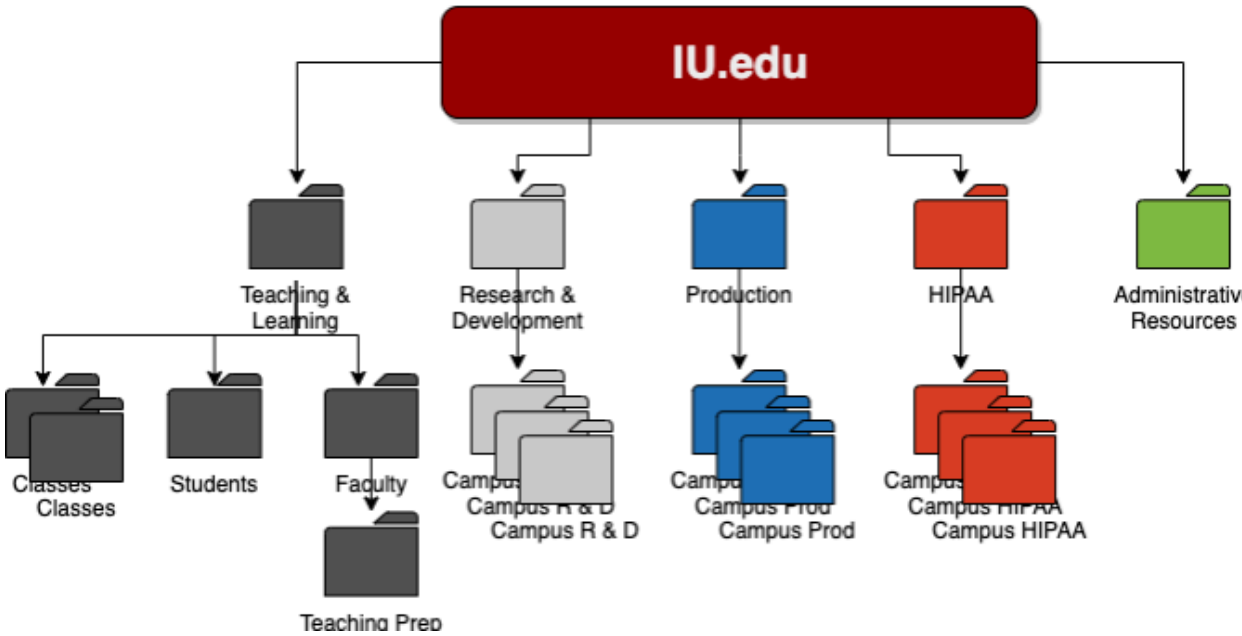
- By decision point
    - Before the contract
        - What homework do you need to do before you start down the road.
            - Do you have the domain?
            - Do you have your identity space nailed down?
            - Who is your primary audience (admin/researchers/students)?
                - How do you plan to allow/offer GCP services to the different populations/use cases?
            - If you don't have G Suite, what are the pros and cons of getting it, if only for identity?
                - Mention of google groups for handling role permissions for projects?
    - Org structure
    - Billing structure
    - Security structure
    - Network structure

- Organization start up
    - Drivers
        - Default GCP Behaviors
            - G Suite environment provides identity to its GCP environment.
            - By default, anyone with an enterprise login can log in to create a project in the associated GCP Org node.
            - Anyone with a project can set up a billing ID.
            - Google gives new "free tier" users $300 in GCP credits when they enter their credit card information to cover cost overruns.
            - Faculty may request teaching credits which students can use without entering credit card info.
            - Google is currently the vendor most engaged and most generous to faculty for teaching.
            - Faculty may request research credits (default $5,000-$20,000) which must be used with Billing IDs tied to the contract. COVID research runs higher.

        - Many projects are abandoned after new user or course credits run out or a course ends.
    - Pertinent Information from NET+ GCP Contract
        - Per contract, <institution> has responsibility for all projects in our GCP Org. <institution> has legal/fiscal liability for some users based on the following distinctions.
            - "ES user" - User working within the scope of their employment. Institution is liable for their actions.
            - "Non-ES user" - User not working within the scope of their employment. No institutional liability.
        - A number of NET+ GCP resellers are approved for the NIH STRIDES program. This is a discount program for NIH-funded researchers.
        - A BAA is available from Google tied to this contract vehicle.
- Structure
    - Org/Folder/Project basics
        - A GCP Org is tied to a G Suite or Google Cloud Identity Domain
            - The value of a sandbox Org
                - What really requires a test org and what just requires good test/dev practices
        - A Folder is both an organizational and a security concept. They are policy and permission frontiers.
        - Projects are conceptual containers or workspaces
        - Resources are the tools and services one leverages to accomplish your objectives



- Where are “accounts”?
    - Accounts in the sense of what a customer is given in your Org to do work on the platform are, in the GCP-verse, a combination of one or more projects and with one or more billing IDs.
- A sample higher ed Org structure might look like this:



-

Networking

[Partner Interconnect: I2 Cloud Connect]: Use regional infrastructure in conjunction with the I2 Network to reach the Google Cloud Platform Dedicated Interconnect.

[GCP Networking Services and Products]
GCP provides options for Hybrid or VPC connectivity like Cloud Interconnect, Cloud VPN, Carrier Peering, Direct Peering, as well as specific VPC services.

Decision Points and Consequences

VPC	INTERCONNECT

Networking Examples

Security

Basic components

- Cloud Security Command Center (CSCC)
- Operations
- Organization Policies
- Forseti

Decision points and consequences

- What to monitor with CSCC
    - Inventory

Security Examples

- TBD

Resources:

- GCP NetSec Training

Support

“Role-based Support” (GCP Documentation Link)

The person with this support role has that role and a view of all support tickets of that level across your entire organization. You can select from four user roles:

- Basic
- Development
- Production
- Business Critical (Enterprise Support only)

Development | Production | Premium

Identity & Access Management

Roles

Roles grant one or more privileges to a user (or members of a group) that allow performing a function within GCP. GCP Documentation provides a good overview of important roles and options: https://cloud.google.com/billing/docs/concepts#roles_overview

Best Practice Recommendations

- Assign GCP roles to Google Groups.
- Adding a user to a group then provides them with the necessary roles/permissions to perform their GCP work.
    - *Note: Ideally you would manage these kinds of access groups automatically through integration with your Identity Management system, so users are moved in/out of groups without manual intervention.*
- For example, create google groups such as:
    - GCP Organizational Admins
    - GCP Billing Admins
    - GCP Student Project Creators
        - Granted the Project Creator role on a “Student Projects” folder only

Other Resources & Information

Internet2 Github

github.internet2.edu

Internet2 maintains a github community for GCP member schools to share code. Everyone has read access, and Internet2 can provide contribute access on request.

UofM TerraForm

https://gitlab.umich.edu/its-inf-cs-terraform-modules/terraform-google-gcp-at-um-project

Training Programs

- Internet2 CLASS
- GCP self-paced training (Google Cloud Skills Boost)
- Online training options
- STRIDES
- GCP NetSec Training