aws

Organizations	dev-syncomint.ca	pat-syncomint.ca		syncomint.ca
OUs	dev	pat	pre-prod	prod
Accounts	dev-mission-cspm	pat-mission-cspm	preprod-mission-cspm	prod-mission-cspm

Resources

```
VPC
  ┌──────────────┐   ┌──────────────┐
  │ Private Subnet│   │ Public Subnet │
  │              │   │   ┌──────┐    │
  │              │   │   │ NAT  │    │
  │              │   │   └──────┘    │
  └──────────────┘   └──────────────┘
       Internet Gateway
```

1. Same design for all the above host projects
2. Note: CIDR for public subnets can be small (/27 or /28) but for private lets use /24
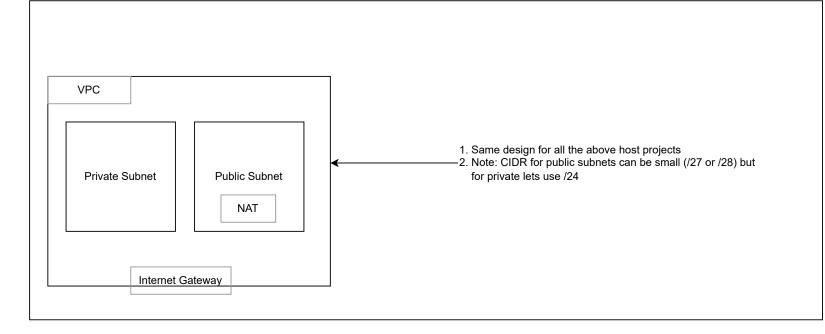
1. 2 basic free-tier if possible VMS in private subnet
2. 2 Storage Buckets
3. 1 Cloud SQL Database [Optional based on cost
4. Same resources for each Project
5 Follow naming conventions

1. Billing estimate for month is needed per org wise
2. Build entire setup using Terraform and modules
3. Use Terraform Cloud [Ask for assess]
4. Code should be in GitHub under Syncomint Org and pipelines should be developed in GH actions for deploying resources
5. Please store secrets as GitHub Secrets that is used for pipeline
3. IAM has to be used and a basic notes should be provided

AWS Policies:
1. 3 Policies for EC2 Instance from (https://cloudsecurityalliance.org/research/cloud-controls-matrix)
2. 2 Policies for S3 from (https://cloudsecurityalliance.org/research/cloud-controls-matrix)
3. 1 IAM Policy from (https://cloudsecurityalliance.org/research/cloud-controls-matrix) should be setup
4. The above policies should be grouped as ccm-controls under AWS/IAM Policy
5. 2 Policies for Compute Engine from FedRAMP Compliance should be implemented
6. 2 Policies for GCS from FedRamp should be implemented
7. The above policies should be grouped as fedramp-controls under AWS/IAM Policy
8. All the above policies should be implemented as code from GitHub and deploying using GH actions pipeline
9. Please identify the above policies in such a way that they can customized and applied for testing using custom policy code