AWS Control Tower Lab Simulation Workbook

1. Introduction

This workbook is designed to help you understand AWS Control Tower, Account Factory, and SCP governance through theory and simulation exercises - without provisioning real AWS accounts.

2. Architecture Simulation

- Draw a layout of an AWS Organization with the following:
  - 3 Organizational Units: Dev, Test, Prod
  - Each OU contains 2-3 AWS accounts
  - Control Tower governance accounts: Audit, Log Archive

- Identify where guardrails (SCPs and Config rules) would apply.
- Determine which services should be enabled in all accounts (e.g., CloudTrail, AWS Config).

3. Account Factory Simulation

- Simulate filling out a request for a new account:
  - Account name: teamX-dev
  - Email: teamX+dev@example.com
  - OU: Dev
  - Enable VPC creation? Yes

- Describe what steps AWS Control Tower will perform after submission.
- Estimate how long provisioning would take and what to check after creation.

4. SCP Policy Practice

- Write an SCP to allow only t3.micro instances:

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "ec2:InstanceType": "t3.micro"
        }
      }
    }
  ]
}
```

- Practice writing SCPs that:
  - Block S3 public access
  - Deny IAM user creation

5. Account Lifecycle Planning

- Describe the lifecycle of an AWS account in an enterprise:
  - Creation -> Use -> Monitoring -> Deactivation -> Quarantine or Archive

- Simulate steps for quarantining an unused account:
  - Move to 'Quarantine OU'
  - Apply SCP that denies all actions
  - Remove IAM permissions
  - Notify owner

6. Useful Resources

- AWS Control Tower Overview: https://docs.aws.amazon.com/controltower/latest/userguide/

- AFT (Account Factory for Terraform): https://docs.aws.amazon.com/controltower/latest/userguide/aft-overview.html

- SCP Examples: https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples.html