Complete WorkFlow AWS config

### **Summary:**

This doc contains structure and plan to implement aws config in any aws account. The below plan will be rolled out in the terraform module.

**Working:**

AWS Config provides a detailed view of the configuration of AWS resources in your AWS account.

**Plan & Structure** :

* Create terraform module to create aws config recorder and delivery channel( s3 bucket)
* Tf module Structure
  + main.tf
    - Contains main tf code invoking resource modules (for eg. config recorder , delivery channel [s3 bucket], rule etc..)
  + vars.tf
    - Variables ( names, tags , region, profile etc..)
  + tfvars.tf
  + modules(dir)
    - delivery-channel.tf
    - aws-config recorder.tf
    - config-aws-managed-rule.tf
    - config-self-managed-rule.tf
    - iam-role-policy.tf
    - Output.tf
* ADO pipeline / tf agent to run tf plan apply
* ADO pipeline / tf agent to destroy aws config

**Access required:**

| **Service** | **User type** | **Iam Access Boundary** | **Reason** | **Iam policy name** |
| --- | --- | --- | --- | --- |
| Create & edit aws config | Service user | Full access | Users who set up and manage AWS Config must have full-access permissions. With full-access permissions, users can provide Amazon S3 and Amazon SNS endpoints that AWS Config delivers data to, create a role for AWS Config, and turn on and turn off recording. | **Config ( Access All Permission )** |
| Use aws config to check | Regular user | Read Only access | With read only aws config access he/she can check compliance / Non compliance | **Config ( Read All Permission )** |

**Action Items:**

* Create & terraform module and test it (half done)
* Create custom config rules (will have to create lambda)
* IAM service role (access all) (create separate tf module)
* IAM user role for read only access ( separate tf module)