***Scenario:-***

1. Scenario: Resource Tagging Compliance

• Your organization mandates that all resources in a specific resource group must be tagged with Environment and CostCenter tags. Design an Azure Policy to enforce this requirement. Ensure that the policy denies the creation of resources that lack these tags.

• Task: Create a policy definition for this requirement, assign it to a resource group, and test it by attempting to create resources without the required tags.

2. Scenario: Restrict Resource Types

• The cloud governance team wants to ensure that only certain virtual machine sizes can be deployed in a specific subscription. For cost optimization, only Standard\_B2s and Standard\_B1s sizes should be allowed.

• Task: Write an Azure Policy that restricts the deployment of virtual machines to only these sizes. Assign it to a subscription and validate the policy by trying to deploy different VM sizes.

3. Scenario: Enforcing Encryption on Storage Accounts

• For compliance purposes, your organization requires that all storage accounts have encryption enabled. Existing storage accounts that are not encrypted should be flagged as non-compliant.

• Task: Define and assign an Azure Policy that audits existing storage accounts for encryption and denies the creation of any new storage accounts without encryption.

4. Scenario: Geo-Location Restriction

• Your organization has a policy that all resources must be deployed only in the East US and West US regions due to data residency requirements.

• Task: Create a policy definition that enforces this restriction on all resource groups in a subscription. Test the policy by attempting to create resources in other regions.

5. Scenario: SQL Database Auditing

• To meet regulatory requirements, you must ensure that all SQL databases have auditing enabled. The policy should ensure that any new SQL database creation has auditing enabled, and existing databases without auditing should be flagged as non-compliant.

• Task: Write a policy that checks for auditing settings on SQL databases. Deploy it at the subscription level and validate its effectiveness by auditing existing and new SQL databases.

6. Scenario: VM Disk Encryption

• To enhance security, your organization requires that all virtual machine disks be encrypted using customer-managed keys. Existing VMs that do not meet this criterion should be reported.

• Task: Create an Azure Policy that audits all VMs for disk encryption using customer-managed keys and prevents the creation of non-compliant VMs.

7. Scenario: Managed Identity Enforcement

• To ensure secure authentication, your company requires that all App Services and Function

***Solution:-***

***1. Resource Tagging Compliance***

\*\*Policy Name\*\*: `Enforce Tags on Resources`

#### Steps to Create the Policy

1. \*\*Create Policy Definition\*\*:

- Go to \*\*Azure Policy\*\* > \*\*Definitions\*\* > \*\*Create policy definition\*\*.

- Define the policy with `"policyRule"` set to check for `Environment` and `CostCenter` tags.

- Set the effect to `Deny` if the tags are missing.

2. \*\*Assign the Policy\*\*:

- Assign it to the specific resource group where this requirement applies.

3. \*\*Test the Policy\*\*:

- Try creating a resource without the `Environment` or `CostCenter` tags. The resource creation should be denied.

#### Verification

- Go to \*\*Azure Policy\*\* > \*\*Compliance\*\* and select the resource group to check for compliance with this policy.

***2. Restrict Resource Types***

\*\*Policy Name\*\*: `Restrict VM Sizes to Standard\_B2s and Standard\_B1s`

#### Steps to Create the Policy

1. \*\*Create Policy Definition\*\*:

- Define a policy with a `"policyRule"` that checks for VM sizes.

- Include conditions to allow only `Standard\_B2s` and `Standard\_B1s` and deny others.

2. \*\*Assign the Policy\*\*:

- Assign it at the subscription level for the specific subscription.

3. \*\*Test the Policy\*\*:

- Attempt to deploy a VM of an unapproved size (e.g., `Standard\_D2s\_v3`). The policy should prevent its creation.

#### Verification

- Check compliance in \*\*Azure Policy\*\* > \*\*Compliance\*\* for the subscription.

***3. Enforcing Encryption on Storage Accounts***

\*\*Policy Name\*\*: `Enforce Storage Account Encryption`

#### Steps to Create the Policy

1. \*\*Create Policy Definition\*\*:

- Define a policy that audits `Microsoft.Storage/storageAccounts`.

- Ensure encryption is enabled for the `encryption.services` property in the policy rule.

- Set `"Deny"` as the effect for new storage accounts without encryption.

2. \*\*Assign the Policy\*\*:

- Assign it at the subscription level.

3. \*\*Test the Policy\*\*:

- Attempt to create a storage account without encryption; the creation should be denied.

#### Verification

- Go to \*\*Azure Policy\*\* > \*\*Compliance\*\* to review non-compliant storage account

***4. Geo-Location Restriction***

\*\*Policy Name\*\*: `Restrict Resources to East US and West US`

Steps to Create the Policy

1. \*\*Create Policy Definition\*\*:

- Define a policy to restrict deployments to `East US` and `West US` regions.

- Use a `"Deny"` effect for resource creation in any other region.

2. \*\*Assign the Policy\*\*:

- Assign it to the subscription level for all resource groups within that subscription.

3. \*\*Test the Policy\*\*:

- Try deploying a resource in a different region (e.g., `Central US`). It should be denied.

#### Verification

- Use \*\*Azure Policy\*\* > \*\*Compliance\*\* to check compliance by region.

***5. SQL Database Auditing***

\*\*Policy Name\*\*: `Enforce SQL Database Auditing`

Steps to Create the Policy

1. \*\*Create Policy Definition\*\*:

- Define a policy that audits SQL databases to check if `auditingPolicy` is enabled.

- Include conditions to flag non-compliant databases.

2. \*\*Assign the Policy\*\*:

- Assign it at the subscription level.

3. \*\*Test the Policy\*\*:

- Create a new SQL database without enabling auditing; it should be flagged as non-compliant.

#### Verification

- Check \*\*Azure Policy\*\* > \*\*Compliance\*\* to review SQL database auditing compliance.

***6. VM Disk Encryption***

\*\*Policy Name\*\*: `Enforce Disk Encryption with Customer-Managed Keys`

#### Steps to Create the Policy

1. \*\*Create Policy Definition\*\*:

- Define a policy to check VM disks for encryption with customer-managed keys.

- Set the effect to `Deny` for non-compliant new VMs.

2. \*\*Assign the Policy\*\*:

- Assign it at the subscription level.

3. \*\*Test the Policy\*\*:

- Try to create a VM without customer-managed disk encryption; it should be denied.

#### Verification

- Use \*\*Azure Policy\*\* > \*\*Compliance\*\* to review VM compliance for disk encryption.

***7. Managed Identity Enforcement***

\*\*Policy Name\*\*: `Enforce Managed Identity on App Services and Functions`

#### Steps to Create the Policy

1. \*\*Create Policy Definition\*\*:

- Define a policy that checks for the presence of a system-assigned managed identity on App Services and Azure Functions.

- Include `"Deny"` as the effect for any resources missing the identity.

2. \*\*Assign the Policy\*\*:

- Assign this policy to the specific resource group or subscription.

3. \*\*Test the Policy\*\*:

- Attempt to create an App Service without a managed identity; it should be denied.

#### Verification

- Check compliance in \*\*Azure Policy\*\* > \*\*Compliance\*\* for identity enforcement on App Services and Functions.