**Handout: Administer Governance and Compliance in Azure (AZ-104 Module)**

**Overview**

This handout covers key concepts, practices, and tools to administer governance and compliance in Azure, based on the "Administer Governance and Compliance" module of the AZ-104 certification. These topics are essential for effectively managing Azure subscriptions, resources, costs, and access using governance tools such as Azure Policy and Role-Based Access Control (RBAC).

**1. Azure Subscriptions and Resource Management**

**Azure Subscription**

* **Definition**: A logical unit of Azure services that serves as a billing and access boundary.
* **Creation**: Only identities in Azure AD or trusted directories can create subscriptions.
* **Types**:
  + **Free**: Includes $200 credit for the first 30 days and limited free access for 12 months.
  + **Pay-As-You-Go**: Charges monthly based on usage.
  + **CSP (Cloud Solution Provider)**: Provides possible discounts through a Microsoft partner.
  + **Enterprise**: Offers enterprise-level discounts for large-scale organizations.

**Resource Groups**

* **Definition**: A container that holds related resources for an Azure solution. Resources in a group should share the same lifecycle and management practices.
* **Features**:
  + Resources in a group can be from different regions.
  + Resource groups cannot be nested.
  + Resources can be moved between groups if needed.

**Service Limits and Quotas**

* Azure resources have default quotas that limit the number of resources a subscription can create or consume.
* These limits help avoid overuse and unexpected costs. Quotas can be increased by submitting support requests if needed.

**Azure Resource Hierarchy**

* **Management Groups**: Provide a higher level of scope above subscriptions. Policies and budgets can be enforced across multiple subscriptions through management groups.

**2. Azure Policy**

**Overview**

* **Azure Policy**: A governance tool that allows you to create, assign, and manage policies to enforce rules over Azure resources.
* **Advantages**:
  + Helps maintain compliance by enforcing policies at scale.
  + Allows for remediation of non-compliant resources.

**Common Use Cases for Azure Policy:**

* **Allowed Resource Types**: Restricts the types of resources that can be deployed.
* **Allowed Locations**: Limits where resources can be deployed geographically.
* **Tagging Compliance**: Enforces the requirement that specific tags are applied to resources for organization and billing purposes.
* **VM SKU Limitations**: Restricts the allowed virtual machine SKUs for deployment.
* **Azure Backup**: Ensures that backup services are enabled for virtual machines.

**Key Steps for Azure Policy:**

1. **Create Policy Definition**: Define the rules and conditions for the policy.
2. **Scope and Assign the Policy**: Apply the policy to a specific scope (management group, subscription, resource group).
3. **Monitor Compliance**: Regularly assess resource compliance with the policy and take corrective action if needed.

**3. Role-Based Access Control (RBAC)**

**Overview**

* **RBAC**: A security model that restricts access to Azure resources based on the roles assigned to users or groups. It ensures users have only the necessary permissions to perform their job functions.

**Key Concepts:**

1. **Security Principal**: An object representing a user, group, or service requesting access to resources.
2. **Role Definition**: A collection of permissions describing the operations that can be performed on Azure resources.
3. **Scope**: Defines the level at which access applies (management group, subscription, resource group, or resource).
4. **Role Assignment**: The process of assigning a role definition to a security principal at a specific scope.

**Built-In RBAC Roles:**

* **Owner**: Full access to all resources, including permission delegation.
* **Contributor**: Can create and manage resources but cannot grant access to others.
* **Reader**: Can view resources but cannot make changes.
* **User Access Administrator**: Manages access to Azure resources but does not manage the resources themselves.

**Custom RBAC Roles:**

* Administrators can create custom roles to provide specific sets of permissions based on organizational needs.

**4. Cost Management and Optimization in Azure**

**Cost Management:**

* **Resource Costs**: Azure services are resource-specific, and costs can vary based on the resource type, region, and usage.
* **Azure Reservations**: Allow organizations to prepay for resources (e.g., VMs or databases) for one or three years, significantly reducing pay-as-you-go costs.
* **Azure Hybrid Benefit**: Provides cost savings for organizations with existing Windows Server or SQL Server licenses, allowing them to apply those licenses to Azure resources.

**Cost Optimization Strategies:**

* **Azure Credits**: Available to developers, students, and enterprise customers for testing and learning.
* **Tagging**: Use resource tags to categorize and roll up billing data by project, department, or cost center.
* **Cost Alerts and Budgets**: Create alerts and budgets to monitor and control resource spending.

**5. Lab 02a - Manage Subscriptions and RBAC**

**Scenario:**

You are tasked with improving the management of Azure resources for Contoso by implementing management groups and granting user permissions for submitting support requests.

**Objectives:**

1. **Implement Management Groups**: Create management groups to organize Azure subscriptions.
2. **Create Custom RBAC Roles**: Define new roles based on specific access requirements.
3. **Assign RBAC Roles**: Assign roles to users and groups to ensure they have appropriate access.

**6. Lab 02b - Manage Governance via Azure Policy**

**Scenario:**

To ensure proper management of infrastructure resources in Contoso, you need to implement governance via Azure Policy.

**Objectives:**

1. **Create and Assign Tags**: Use the Azure portal to create tags and enforce them on resources.
2. **Enforce Tagging via Policy**: Create policies that require specific tags on resources.
3. **Remediate Non-Compliant Resources**: Ensure that non-compliant resources are brought into compliance using policy remediation.

**7. Lab 03a - Manage Azure Resources with the Azure Portal**

**Scenario:**

You need to explore Azure resource administration capabilities, such as organizing resources by groups, moving resources between groups, and protecting resources using resource locks.

**Objectives:**

1. **Create Resource Groups**: Group related Azure resources for simplified management.
2. **Move Resources**: Move resources between different resource groups as required.
3. **Implement and Test Resource Locks**: Prevent accidental deletion of critical resources by applying resource locks.

**Summary**

Azure governance and compliance features are essential tools for managing cloud resources effectively. Azure subscriptions, policies, RBAC, and cost management strategies help maintain control, security, and compliance across multiple Azure environments.

Reference links

<https://docs.microsoft.com/azure/cost-management-billing/manage/create-subscription>

<https://docs.microsoft.com/azure/governance/policy/overview>

<https://docs.microsoft.com/azure/role-based-access-control/overview>

A list of regions and their locations is available at <https://azure.microsoft.com/global-infrastructure/locations/>

Here is a link to the list of regional pairs: <https://learn.microsoft.com/azure/reliability/cross-region-replication-azure#azure-cross-region-replication-pairings-for-all-geographies>

Microsoft datacenters animation - <https://datacenters.microsoft.com/globe/explore>

Virtual datacenter tour - <https://datacenters.microsoft.com/globe/explore/datacenter>

Create an additional Azure subscription - <https://docs.microsoft.com/azure/cost-management-billing/manage/create-subscription>

Change your Azure subscription to a different offer - <https://docs.microsoft.com/azure/cost-management-billing/manage/switch-azure-offer>

Subscription considerations and recommendations - <https://learn.microsoft.com/azure/cloud-adoption-framework/ready/landing-zone/design-area/resource-org-subscriptions>

Organize and manage multiple Azure subscriptions **-** <https://learn.microsoft.com/azure/cloud-adoption-framework/ready/azure-best-practices/organize-subscriptions>

Create management groups for resource organization and management - <https://docs.microsoft.com/azure/governance/management-groups/create>

Manage your resources with management groups - <https://docs.microsoft.com/azure/governance/management-groups/manage>

**Azure usage charges** - https://docs.microsoft.com/azure/billing/billing-understand-your-invoice

Resource naming and tagging decision guide - <https://docs.microsoft.com/azure/cloud-adoption-framework/decision-guides/resource-tagging>

[**https://docs.microsoft.com/azure/governance/policy/overview**](https://docs.microsoft.com/azure/governance/policy/overview)

[**https://docs.microsoft.com/azure/governance/policy/tutorials/create-and-manage**](https://docs.microsoft.com/azure/governance/policy/tutorials/create-and-manage)

**List role definitions in Azure RBAC -** [**https://docs.microsoft.com/azure/role-based-access-control/role-definitions-list**](https://docs.microsoft.com/azure/role-based-access-control/role-definitions-list)

**Add or remove role assignments using Azure RBAC and the Azure portal -** [**https://docs.microsoft.com/azure/role-based-access-control/role-assignments-portal**](https://docs.microsoft.com/azure/role-based-access-control/role-assignments-portal)

**Manage access to an Azure subscription by using Azure role-based access control -** [**https://docs.microsoft.com/learn/modules/manage-subscription-access-azure-rbac/3-elevate-your-access-user-access-admin**](https://docs.microsoft.com/learn/modules/manage-subscription-access-azure-rbac/3-elevate-your-access-user-access-admin)