Introduction to Azure Policies

Azure Policies overview

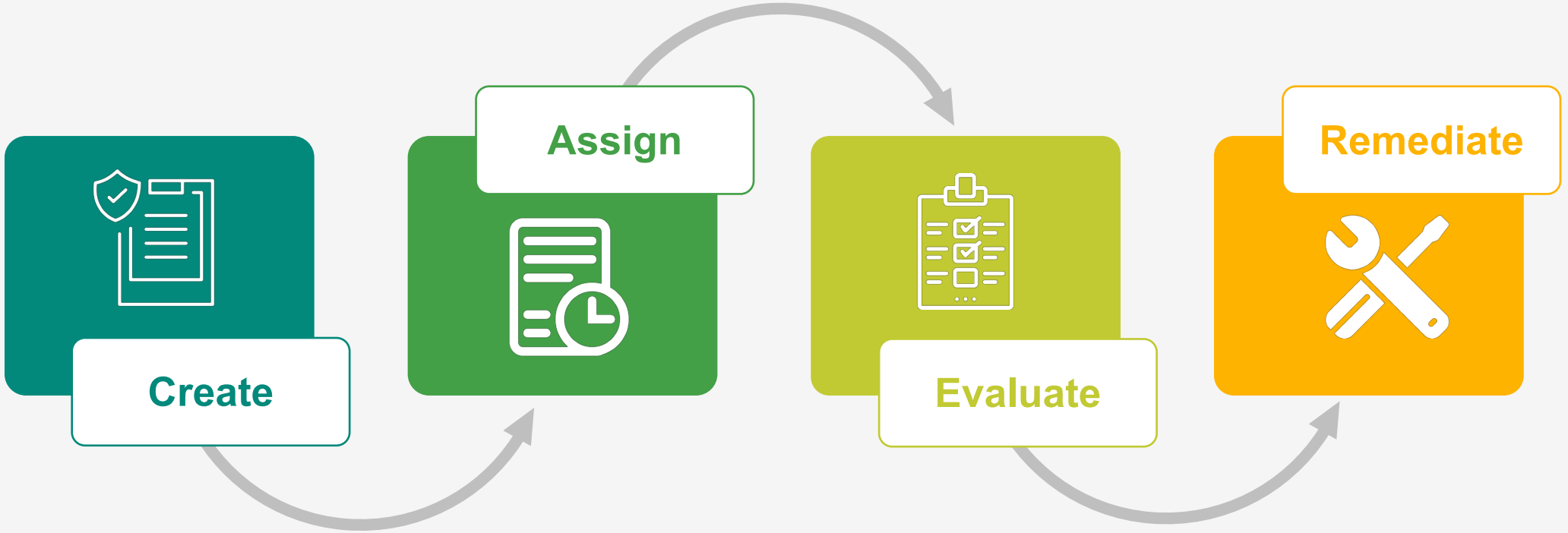
Azure Policy is a service in Azure that you use to create, assign, and manage policies. These policies enforce different rules and effects over your resources, so those resources stay compliant with your corporate standards and service level agreements.

Azure policies Vs RBAC

- RBAC controls user actions at different scopes.
  Example is start and stop virtual machine

- Policy enforce rules on resource properties during deployment and for existing resources.
  Example is to deploy resources at a specific location only

Azure Policy steps



Policy definition has conditions under which it's enforced. And, it has a defined effect that takes place if the conditions are met

A **policy assignment** is a policy definition that has been assigned to take place within a specific scope. This scope could range from a management group to a resource group.

Evaluations of assigned policies and initiatives happen as the result of various events. For e.g. creation of a resource, policy assignment to a scope etc.

Each policy definition in Azure Policy has a single effect. That **effect** determines what happens when the policy rule is evaluated to match

Policy definition

You use JSON to create a policy definition. The policy definition contains elements for:

- Mode – Determines which resource types will be evaluated for the policy
- Parameters - Parameters help simplify your policy management by reducing the number of policy definitions.
- Display name & Description
- Policy rule
    - Logical evaluation
    - Effect

Policy effects

There are currently six effects that are supported in a policy definition:

- **Append** - Append is used to add additional fields to the requested resource during creation or update. For e.g. tags.
- **Audit** - Audit is used to create a warning event in the activity log when evaluating a non-compliant resource, but it doesn't stop the request.
- **AuditIfNotExists** - AuditIfNotExists enables auditing on resources that match the if condition, but doesn't have the components specified in the details of the then condition.
- **Deny** - Deny is used to prevent a resource request that doesn't match defined standards through a policy definition and fails the request.
- **DeployIfNotExists** - Similar to AuditIfNotExists, DeployIfNotExists executes a template deployment when the condition is met.
- Disabled

Initiatives

- **Initiative definition**
  - An initiative definition is a collection of policy definitions that are tailored towards achieving a singular overarching goal. Initiative definitions simplify managing and assigning policy definitions
- **Initiative assignment**
  - Like a policy assignment, an initiative assignment is an initiative definition assigned to a specific scope. Initiative assignments reduce the need to make several initiative definitions for each scope.