Azure Policy
Governance as Code

Joshua Donovan | Azure Support | /josh-donovan

Updated: 05/10/2023

Azure Policy
Governance as Code

Today we are going to discuss:

- What is Azure Policy?
- Azure Policy as a Policy Creator
  - How to understand and write policy. (with demo)
- Azure Policy as someone effected by a Policy
  - How to understand the error, and troubleshoot. (with demo)

What is Azure Policy?

One giant if → then statement.

What is Azure Policy? Continued

- ~~One giant if → then statement.~~ (Yes… but so much more)
- Azure Policy helps to enforce organizational standards and to assess compliance at-scale.
- Azure Policy manages the what and the where of your Azure Environment.
  (RBAC is concerned with who)
- Azure Policy runs on the ARM layer and cannot manage application data (mostly)
- Useful governance Actions
  - Ensuring your team deploys Azure resources only to allowed regions
  - Enforcing the consistent application of taxonomic tags
  - Requiring resources to send diagnostic logs to a Log Analytics workspace

https://learn.microsoft.com/en-us/azure/governance/policy/overview

https://learn.microsoft.com/en-us/azure/role-based-access-control/overview

Azure Policy: Two perspectives

Azure Policy Creator

- Policy Structure
  - Definitions
  - Assignments
  - Exemptions
- What is Remediation?

Resource Effected

- Troubleshooting deployments denied by Policy

Azure Policy Creator

Azure Policy Definition

Policy definitions describe resource compliance conditions and the effect to take if a condition is met.

By defining conventions, you can control costs and more easily manage your resources.

The Policy Definition is where we implement our if → then statement.

Azure Policy Assignment

Policy assignments are used by Azure Policy to define which resources are assigned which policies or initiatives.

The policy assignment can determine the values of parameters for that group of resources at assignment time, making it possible to reuse policy definitions that address the same resource properties with different needs for compliance.

Azure Policy Exemption

-Optional-

The Azure Policy exemptions feature is used to exempt a resource hierarchy or an individual resource from evaluation of initiatives or definitions. Resources that are exempt count toward overall compliance but can't be evaluated or have a temporary waiver.

Build

Enforce

Flexible

Azure Policy Creator

Azure Policy Definition

```
{
    "properties": {
        "displayName": "Allowed locations",
        "description": "This policy enables you to restrict the locations your organization can specify when deploying resources.",
        "mode": "Indexed",
        "metadata": {
            "version": "1.0.0",
            "category": "Locations"
        },
        "parameters": {
            "allowedLocations": {
                "type": "array",
                "metadata": {
                    "description": "The list of locations that can be specified when deploying resources",
                    "strongType": "location",
                    "displayName": "Allowed locations"
                },
                "defaultValue": [ "westus2" ]
            }
        },
        "policyRule": {
            "if": {
                "not": {
                    "field": "location",
                    "in": "[parameters('allowedLocations')]"
                }
            },
            "then": {
                "effect": "deny"
            }
        }
    }
}
```

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effects

Azure Policy Creator

Policy Rule, Logical Operators & Conditions | Azure Policy Definition

```
{
    "if": {
        <condition> | <logical operator>
    },
    "then": {
        "effect": "deny | audit | modify | append | auditIfNotExists | deployIfNotExists | disabled | (preview) denyAction"
    }
}
```

```
"if": {
    "allOf": [
        {
            "not": {
                "field": "tags",
                "containsKey": "application"
            }
        },
        {
            "field": "type",
            "equals": "Microsoft.Storage/storageAccounts"
        }
    ]
},
```

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effects

Azure Policy Creator

Policy Rule & Effects | Azure Policy Definition

```
{
    "if": {
        <condition> | <logical operator>
    },
    "then": {
        "effect": "disabled | modify | append | deny | audit | auditIfNotExists | deployIfNotExists | (preview) denyAction"
    }
}
```

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effects

Azure Policy Creator

Policy Rule & Effects: Modify & Append | Azure Policy Definition

```
| --------- append --------- |

"then": {
    "effect": "append",
    "details": [{
        "field": "Microsoft.Storage/storageAccounts/networkAcls.ipRules",
        "value": [{
            "action": "Allow",
            "value": "134.5.0.0/21"
        }]
    }]
}
```

```
| --------- modify --------- |

"then": {
    "effect": "modify",
    "details": {
        "roleDefinitionIds": [
            "/providers/microsoft.authorization/roleDefinitions/17d1049b-9a84-46fb-8f53-869881c3d3ab"
        ],
        "conflictEffect": "audit",
        "operations": [
            {
                "condition": "[greaterOrEquals(requestContext().apiVersion, '2019-04-01')]",
                "operation": "addOrReplace",
                "field": "Microsoft.Storage/storageAccounts/allowBlobPublicAccess",
                "value": false
            }
        ]
    }
}
```

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effects

Azure Policy Creator

Policy Rule & Effects: AINE | Azure Policy Definition

```
| --------- AuditIfNotExists (AINE) --------- |

{
    "if": {
        "field": "type",
        "equals": "Microsoft.Compute/virtualMachines"
    },
    "then": {
        "effect": "auditIfNotExists",
        "details": {
            "type": "Microsoft.Compute/virtualMachines/extensions",
            "existenceCondition": {
                "allOf": [{
                        "field": "Microsoft.Compute/virtualMachines/extensions/publisher",
                        "equals": "Microsoft.Azure.Security"
                    },
                    {
                        "field": "Microsoft.Compute/virtualMachines/extensions/type",
                        "equals": "IaaSAntimalware"
                    }
                ]
            }
        }
    }
}
```

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effects

Azure Policy Creator

Policy Rule & Effects: DINE | Azure Policy Definition

```
| --------- DeployIfNotExists (DINE) --------- |

"if": {
    "field": "type",
    "equals": "Microsoft.Sql/servers/databases"
},
"then": {
    "effect": "DeployIfNotExists",
    "details": {
        "type": "Microsoft.Sql/servers/databases/transparentDataEncryption",
        "name": "current",
        "evaluationDelay": "AfterProvisioning",
        "roleDefinitionIds": [
            "/subscriptions/{subscriptionId}/providers/Microsoft.Authorization/roleDefinitions/{roleGUID}",
            "/providers/Microsoft.Authorization/roleDefinitions/{builtinroleGUID}"
        ],
        "existenceCondition": {
            "field": "Microsoft.Sql/transparentDataEncryption.status",
            "equals": "Enabled"
        },
        "deployment": {
            "properties": {
                "mode": "incremental",
                "template": {
                    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
                    "contentVersion": "1.0.0.0",
                    "parameters": {
                        "fullDbName": {
                            "type": "string"
                        }
                    },
                    "resources": [
                        {
                            "name": "[concat(parameters('fullDbName'), '/current')]",
                            "type": "Microsoft.Sql/servers/databases/transparentDataEncryption",
                            "apiVersion": "2014-04-01",
                            "properties": {
                                "status": "Enabled"
                            }
                        }
                    ]
                },
                "parameters": {
                    "fullDbName": {
                        "value": "[field('fullName')]"
                    }
                }
            }
        }
    }
}
```

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effects

Azure Policy Creator

Azure Policy Assignment

```
{
    "properties": {
        "displayName": "Enforce resource naming rules",
        "description": "Force resource names to begin with DeptA and end with -LC",
        "metadata": {
            "assignedBy": "Cloud Center of Excellence"
        },
        "enforcementMode": "DoNotEnforce",
        "notScopes": [],
        "policyDefinitionId": "/subscriptions/{mySubscriptionID}/providers/Microsoft.Authorization/policyDefinitions/ResourceNaming",
        "nonComplianceMessages": [
            {
                "message": "Resource names must start with 'DeptA' and end with '-LC'."
            }
        ],
        "parameters": {
            "prefix": {
                "value": "DeptA"
            },
            "suffix": {
                "value": "-LC"
            }
        },
        "identity": {
            "type": "SystemAssigned"
        },
        "resourceSelectors": [],
        "overrides": []
    }
}
```

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/assignment-structure

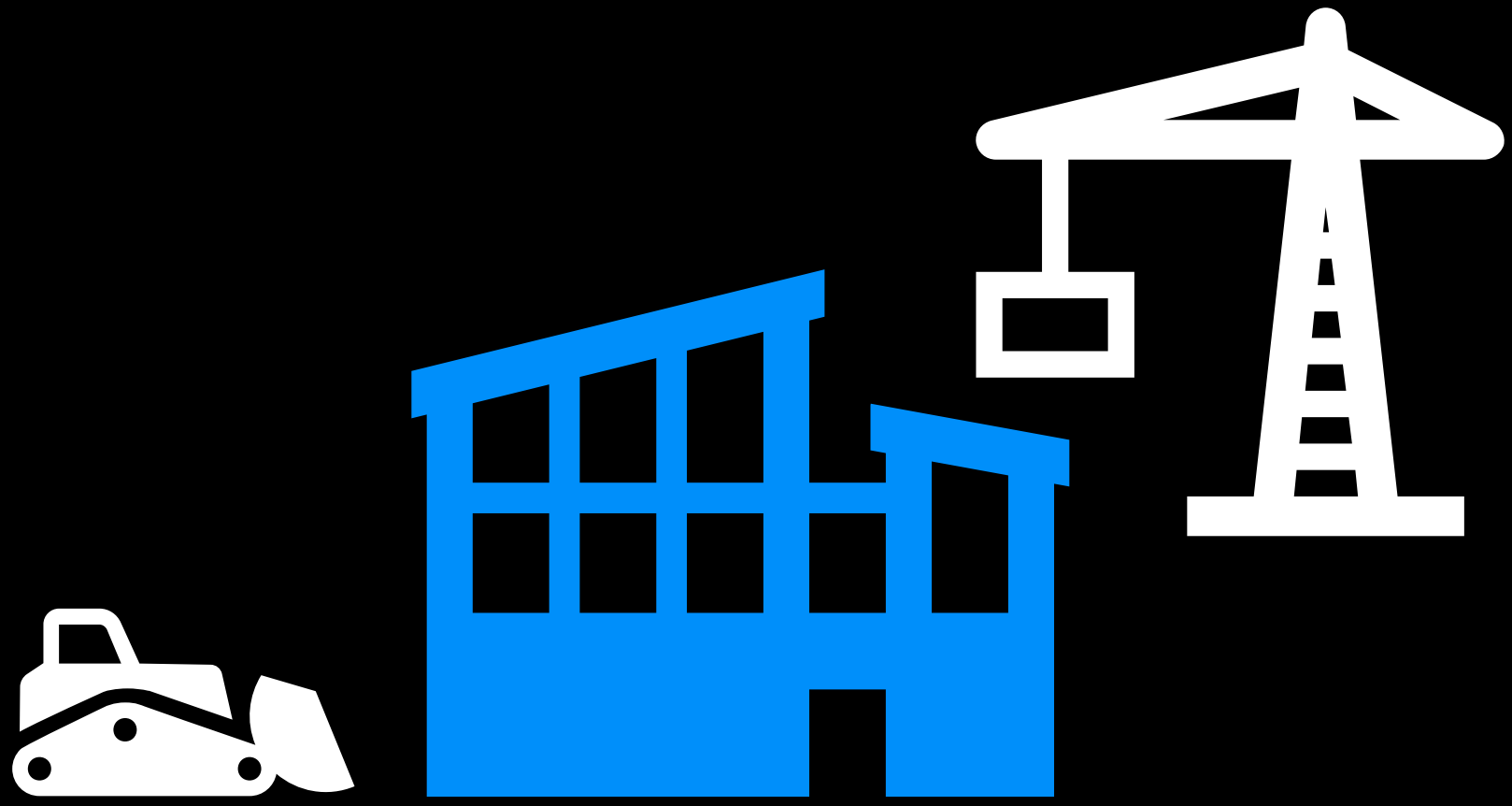
Azure Policy Creator

Azure Policy Exemption

```
{
    "id": "/subscriptions/{subId}/resourceGroups/ExemptRG/providers/Microsoft.Authorization/policyExemptions/resourceIsNotApplicable",
    "apiVersion": "2020-07-01-preview",
    "name": "resourceIsNotApplicable",
    "type": "Microsoft.Authorization/policyExemptions",
    "properties": {
        "displayName": "This resource is scheduled for deletion",
        "description": "This resources is planned to be deleted by end of quarter and has been granted a waiver to the policy.",
        "metadata": {
            "requestedBy": "Storage team",
            "approvedBy": "IA",
            "approvedOn": "2020-07-26T08:02:32.0000000Z",
            "ticketRef": "4baf214c-8d54-4646-be3f-eb6ec7b9bc4f"
        },
        "policyAssignmentId": "/subscriptions/{mySubscriptionID}/providers/Microsoft.Authorization/policyAssignments/resourceShouldBeCompliantInit",
        "policyDefinitionReferenceIds": [
            "requiredTags",
            "allowedLocations"
        ],
        "exemptionCategory": "waiver",
        "expiresOn": "2020-12-31T23:59:00.0000000Z",
        "assignmentScopeValidation": "Default"
    }
}
```

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/exemption-structure

Azure Policy Creator



Create and Assign Policy (in the portal)

DEMO

Azure Policy Creator

Create a Policy
DEMO

Business Requirements [intent]

- We need all Azure KeyVault Network Access Control Lists (ACL) to contain Contoso's IP CIDR ranges.
- This business rule needs to include the production Azure subscription for the Sales department.
- We want to ensure these CIDR ranges are present, but we do not want to restrict others from being added.

https://github.com/Joshua-Donovan/Azure-Policy-Examples/blob/main/Microsoft.KeyVault/vaults/networkAcls/.ipRules/README_noLoops.md

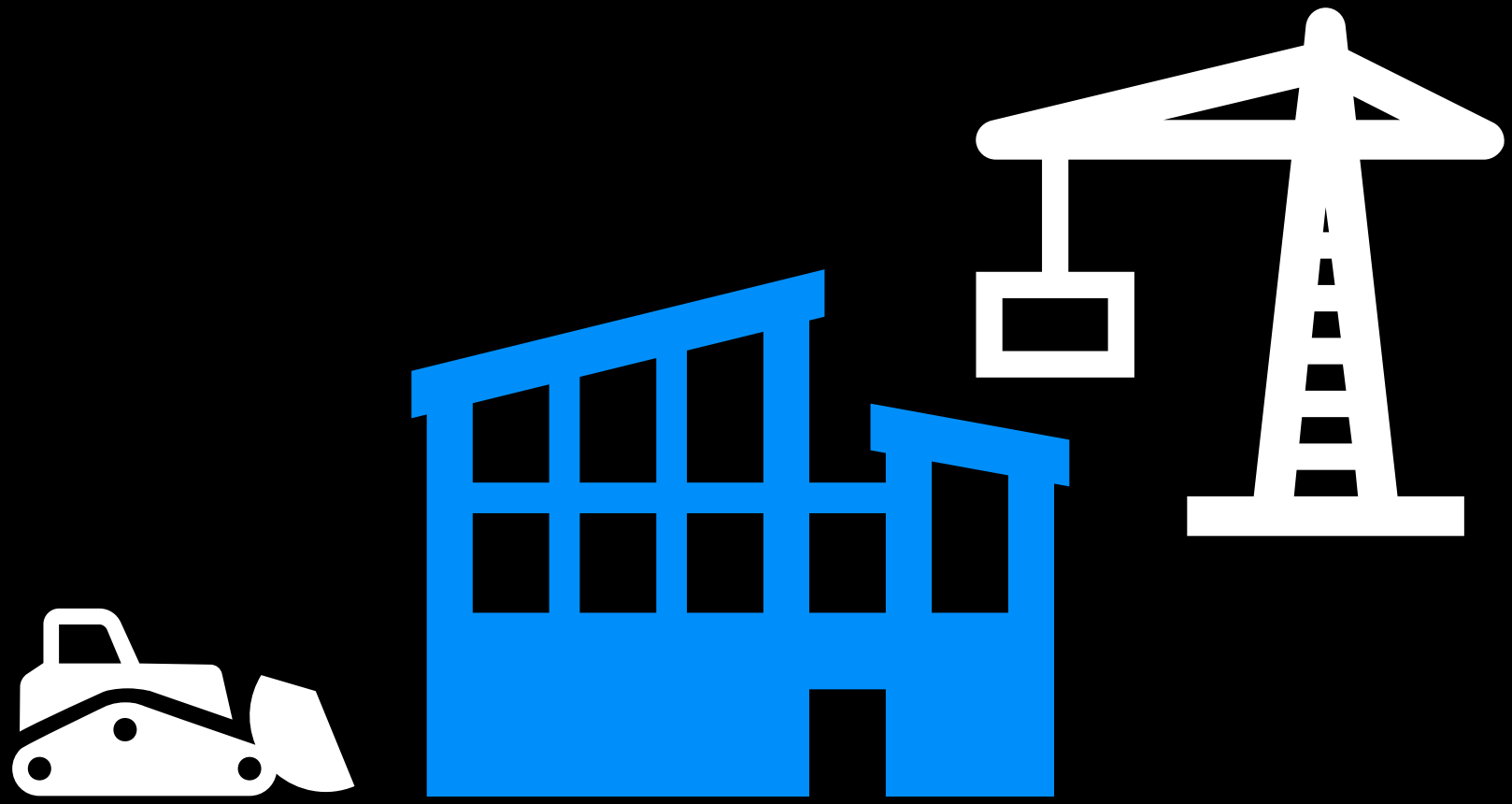
Azure Policy Creator

Azure Policy Remediation

```
{
    "id": "/subscriptions/{subId}/resourceGroups/ExemptRG/providers/Microsoft.PolicyInsights/remediations/remediateNotCompliant",
    "apiVersion": "2021-10-01",
    "name": "remediateNotCompliant",
    "type": "Microsoft.PolicyInsights/remediations",
    "properties": {
        "policyAssignmentId": "/subscriptions/{mySubscriptionID}/providers/Microsoft.Authorization/policyAssignments/resourceShouldBeCompliantInit",
        "policyDefinitionReferenceIds":  "requiredTags",
        "resourceCount": 42,
        "parallelDeployments": 6,
        "failureThreshold": {
            "percentage": 0.1
        }
    }
}
```

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/remediation-structure

Azure Policy Creator



Remediate a Resource

DEMO

Azure Policy Creator

Helpful Links

- Policy Concepts and Docs:
  - https://learn.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure
  - https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effects
  - https://learn.microsoft.com/en-us/azure/governance/policy/concepts/scope
  - https://learn.microsoft.com/en-us/azure/governance/policy/concepts/initiative-definition-structure
  - https://learn.microsoft.com/en-us/azure/governance/policy/concepts/assignment-structure
  - https://learn.microsoft.com/en-us/azure/governance/policy/concepts/exemption-structure
  - https://learn.microsoft.com/en-us/azure/governance/policy/concepts/remediation-structure
    - https://learn.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources
  - … the rest of the concepts section is also good ☺

- Azure Built-In Policies Repository:
  - https://github.com/Azure/azure-policy#resource-management-that-bypasses-azure-resource-manager
- Azure Community Policies Repository:
  - https://github.com/Azure/Community-Policy/
- AzPolicyAdvertizer
  - https://www.azadvertizer.net/azpolicyadvertizer_all.html#%7B%7D

Resource Effected

Deployment denied by Policy

- **Identify** if Policy is what caused your deployment failure, or if it is a general error.
  - If your deployment is denied by Azure Policy you will be returned an error with either a generated error from the policy engine or a **nonComplianceMessages** set by who assigned the policy.

```
Resource 'LoadBalancer_Pub_Prod' was disallowed by policy. (Code:
RequestDisallowedByPolicy)

  Policy: DENY - LoadBalancer with public IP
```


```
5       {
6         "code": "RequestDisallowedByPolicy",
7         "target": "LoadBalancer_ToBeAtAllOther_LoadBalancers",
8         "message": "Resource
    'LoadBalancer_ToBeAtAllOther_LoadBalancers' was disallowed
    by policy. Policy identifiers: '[{\"policyAssignment\":
    {\"name\":\"DENY - LoadBalancer with public IP\",\"id\":\"/
    subscriptions/9b7e76e6-1c02-4e83-bf8f-7509a3dd1aab/
    resourceGroups/Policy_Play/providers/Microsoft.
    Authorization/policyAssignments/4e72f6ef2d7749faa2716326\"},
    \"policyDefinition\":{\"name\":\"DENY - LoadBalancer with
    public IP\",\"id\":\"/subscriptions/
    9b7e76e6-1c02-4e83-bf8f-7509a3dd1aab/providers/Microsoft.
    Authorization/policyDefinitions/
    3bf577b4-98ba-45d6-9465-d048d643257d\"}}]'.",
```


```
Resource 'LoadBalancer_ToBeAtAllOther_LoadBalancers' was
disallowed by policy. (Code: RequestDisallowedByPolicy)

  Policy: DENY - LoadBalancer with public IP
    Reason: You were blocked by the Cloud Team Wizards
```


```
{
  "code": "InvalidTemplateDeployment",
  "message": "The template deployment failed because of
policy violation. Please see details for more information.",
  "details": [
    {
      "code": "RequestDisallowedByPolicy",
      "target": "LoadBalancer_ToBeAtAllOther_LoadBalancers",
      "message": "Resource
'LoadBalancer_ToBeAtAllOther_LoadBalancers' was disallowed
by policy. Reasons: 'You were blocked by the Cloud Team
Wizards'. See error details for policy resource IDs.",
```

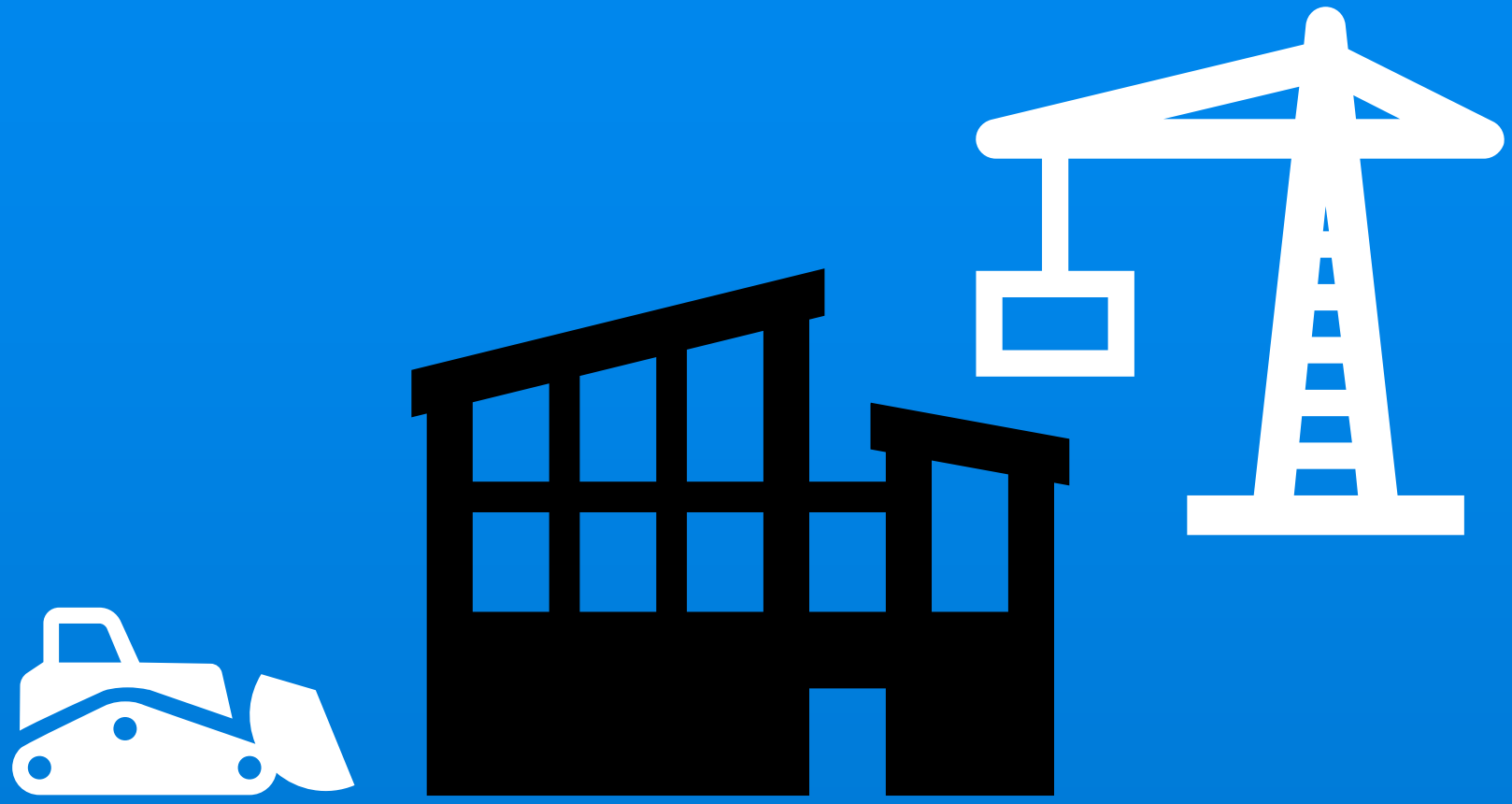

- **Determine** what caused a non-compliant result.
  - If you do not have access to review the policy definition, you may need to contact the department or person that manages Azure Policy in your organization.

- **Update** your deployment to be compliant with the policy (or ask for / deploy an exemption)

https://learn.microsoft.com/en-us/azure/governance/policy/how-to/determine-non-compliance

Resource Effected

Deployment denied by Policy



Troubleshoot a Deny
DEMO

Azure Policy
Governance as Code

Summary:

- What is Azure Policy?
- Azure Policy as a Policy Creator
  - How to understand and write policy. (with demo)
- Azure Policy as someone effected by a Policy
  - How to understand the error, and troubleshoot. (with demo)

Thank you!

Tulsa .NET User Group | 05/11/2023

Slides available on GitHub:
https://github.com/Joshua-Donovan/Slides

Questions?

Joshua Donovan | Azure Support | /josh-donovan