

Azure Governance

Damian Flynn
MVP / Innofactor
@Damian_Flynn

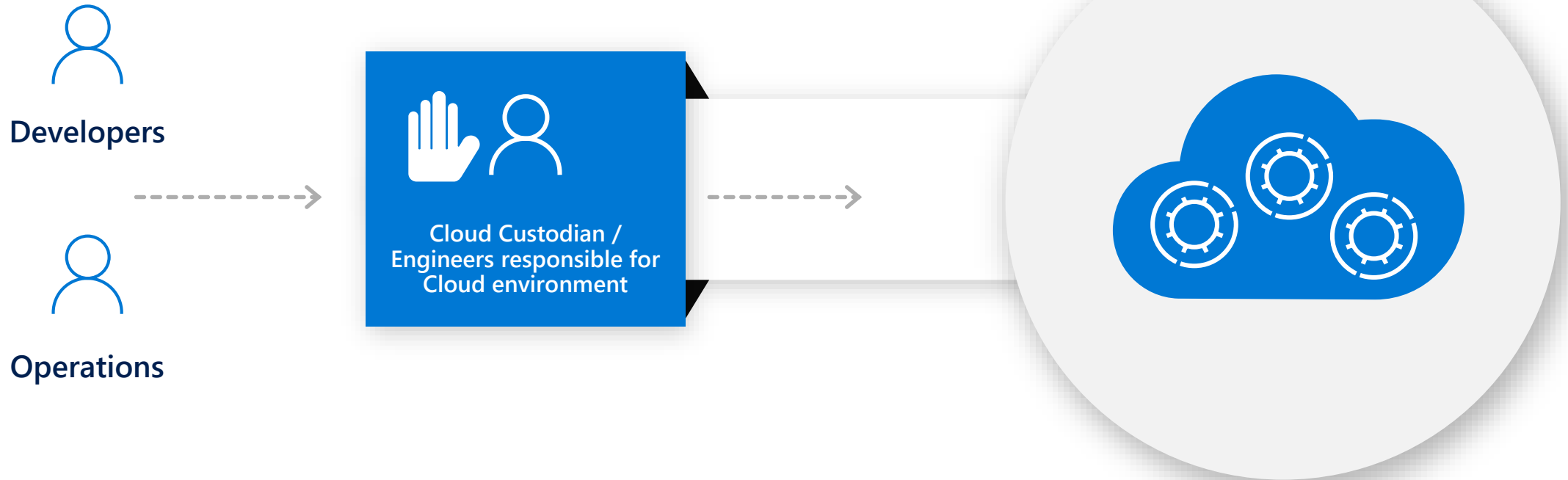
Platinum Sponsor 2019



Microsoft

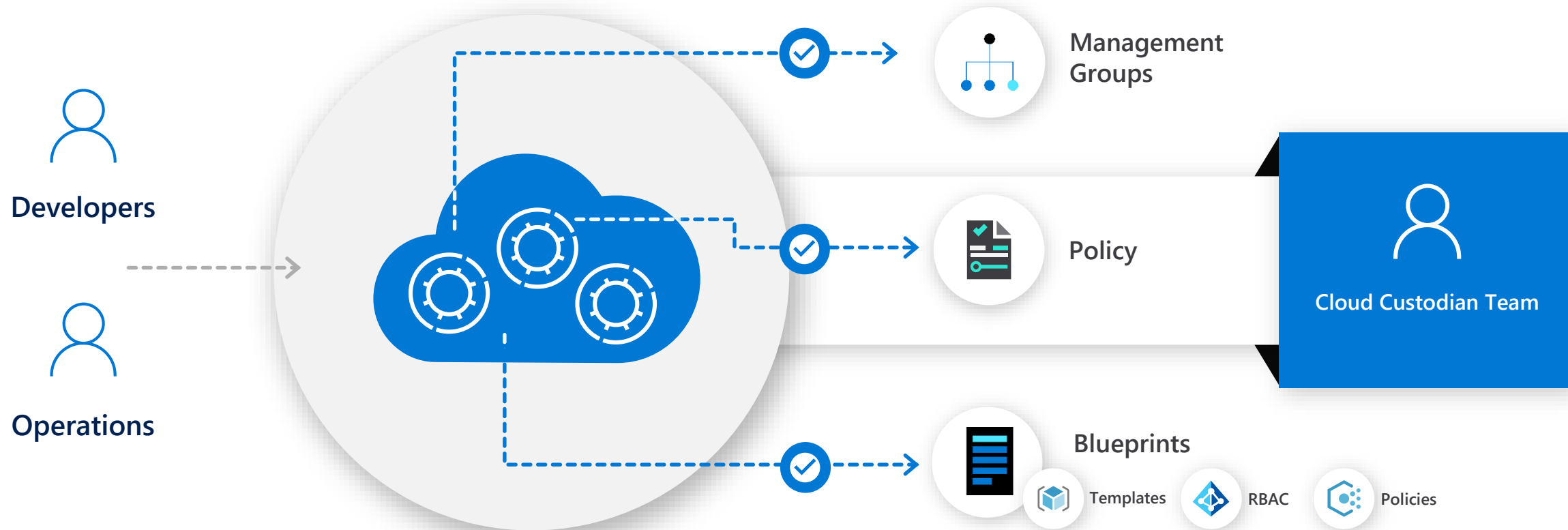
Traditional approach

Block Dev/Ops from directly accessing the cloud (portal/api/cli) to attain control



SPEED + CONTROL

Cloud-native governance -> removing barriers to compliance and enabling velocity





Governance for the cloud

Native platform capabilities to ensure compliant use of cloud resources



Policy

Real-time enforcement, compliance assessment and remediation

Control



NEW

Blueprints

Deploy and update cloud environments in a repeatable manner using composable artifacts

Environment

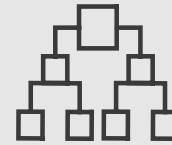


NEW

Resource Graph

Query, explore & analyze cloud resources at scale

Visibility



Management Group

Define organizational hierarchy

Hierarchy



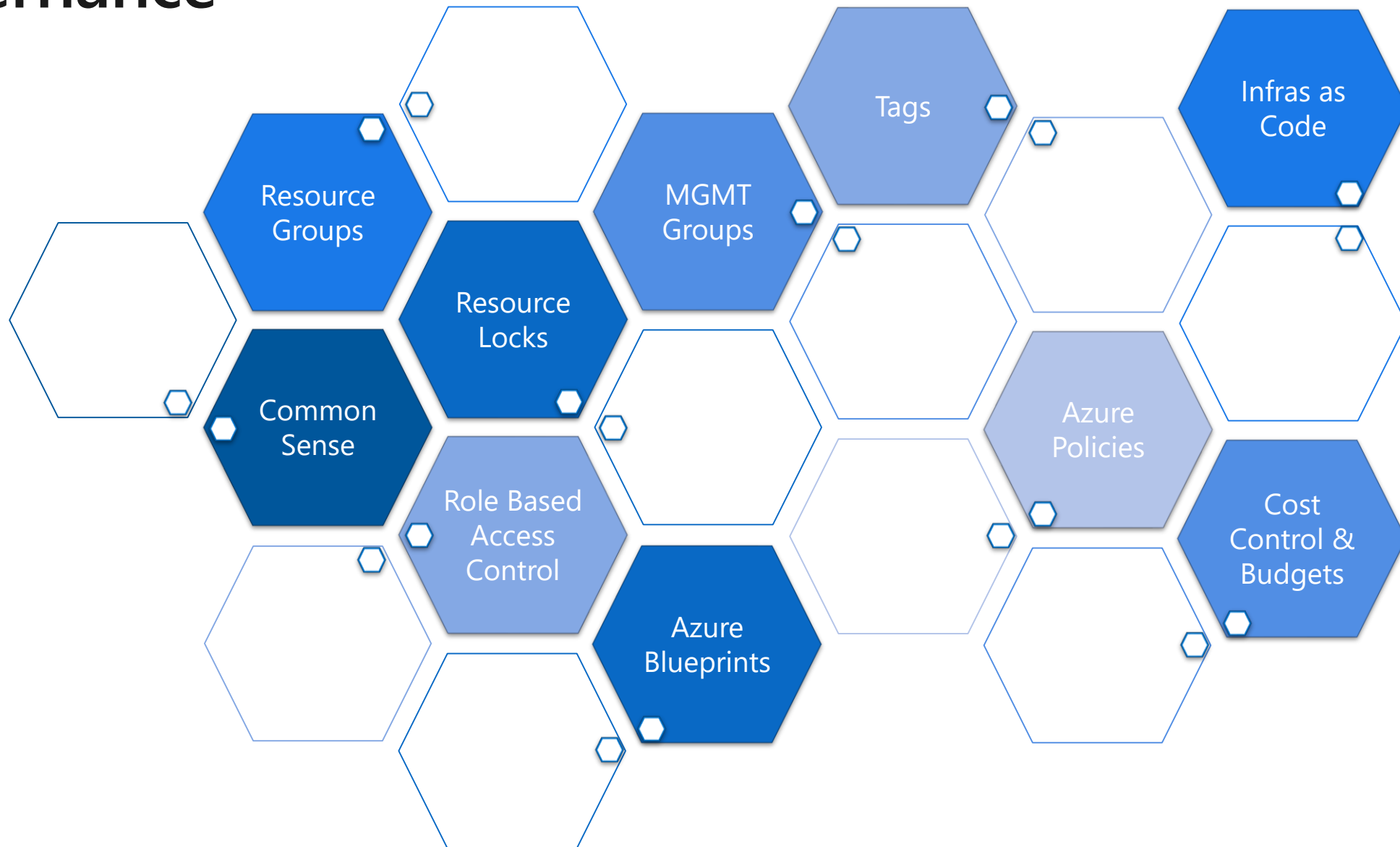
NEW

Cost

Monitor cloud spend and optimize resources

Consumption

Governance

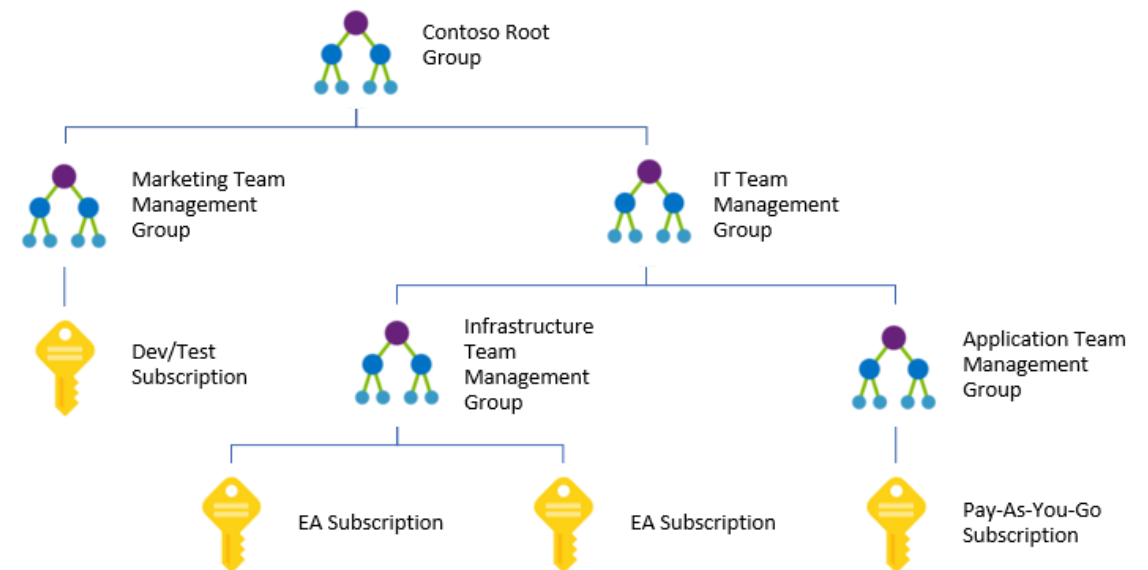


Management Groups

Grouping of subscriptions and managing hierarchy

Management Group best practices

- Define your hierarchy based on organization and environment type (prod, pre-prod, etc.)
- The root MG is for global configuration
 - Be careful with MG level assignments as they will cascade through large chunks of your hierarchy
- Try not to repeat yourself.
 - Assign common policies and RBAC higher up in your hierarchy
- March ETA for custom roles for management groups
- Built-in RBAC roles for MGs (MG contributor, MG reader)
 - Need subscription owner access to move to another MG

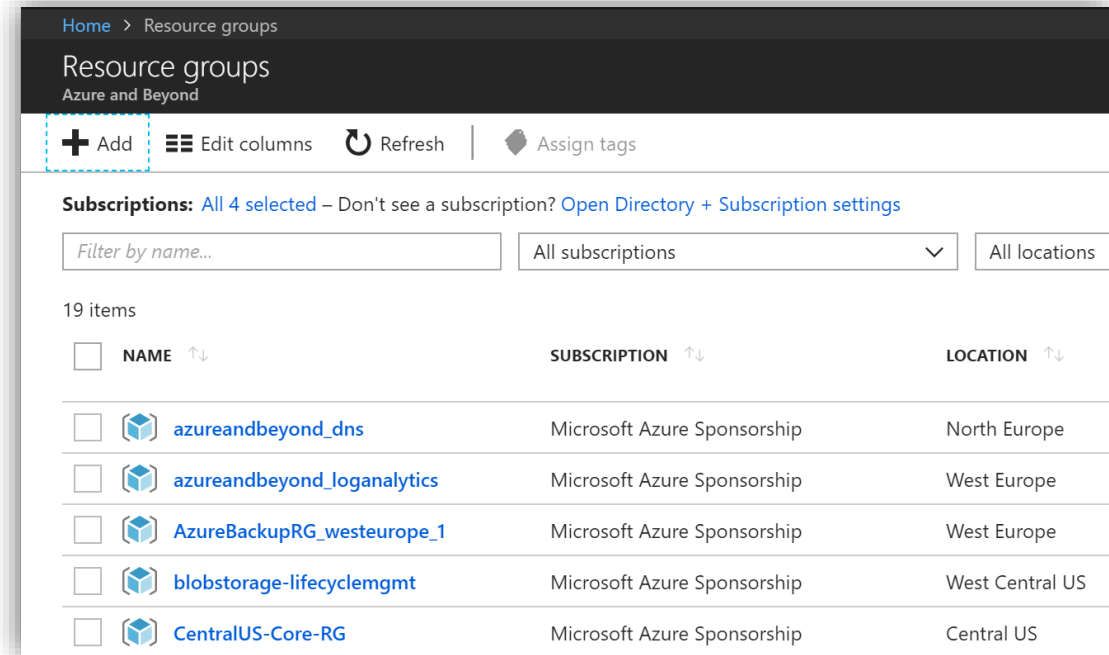


Resource Groups

Grouping of resources and access management

Resource groups

- Management
- Host resources in the same deployment lifecycle
- Assigned to a region but can contain resources that reside in different regions
- Every resource can only exist in one Resource Group
- Resources can be moved between Resource Groups



Home > Resource groups

Resource groups






Azure and Beyond

+ Add Edit columns Refresh Assign tags

Subscriptions: All 4 selected – Don't see a subscription? [Open Directory + Subscription settings](#)

Filter by name... All subscriptions All locations

19 items

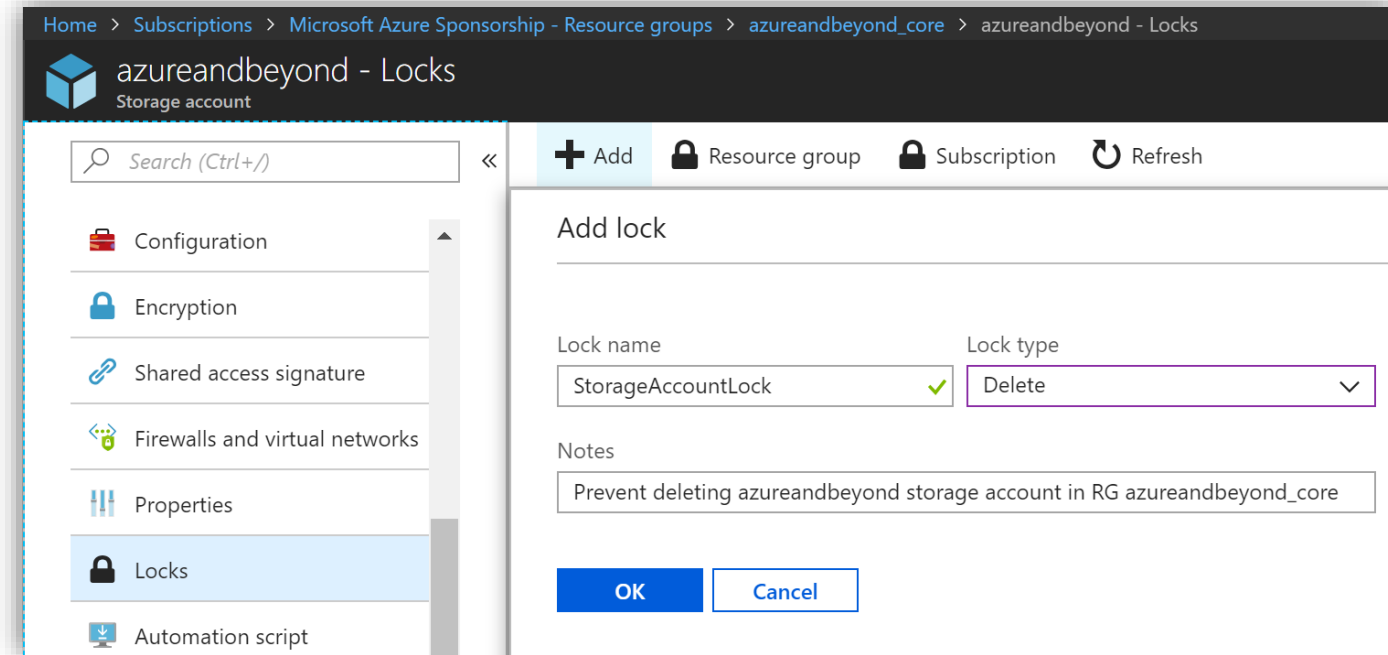
<input type="checkbox"/>	NAME ↑↓	SUBSCRIPTION ↑↓	LOCATION ↑↓
<input type="checkbox"/>	 azureandbeyond_dns	Microsoft Azure Sponsorship	North Europe
<input type="checkbox"/>	 azureandbeyond_loganalytics	Microsoft Azure Sponsorship	West Europe
<input type="checkbox"/>	 AzureBackupRG_westeurope_1	Microsoft Azure Sponsorship	West Europe
<input type="checkbox"/>	 blobstorage-lifecyclemgmt	Microsoft Azure Sponsorship	West Central US
<input type="checkbox"/>	 CentralUS-Core-RG	Microsoft Azure Sponsorship	Central US

Resource Locks

Protecting Resources for Common Sense

Resource locks

- Define your hierarchy based on organization and environment type (prod, pre-prod, etc.)
- Locks protect resources
 - Delete locks
 - ReadOnly locks
- Define locks in advance
- Use them in combination with common sense (e.g. read only means read only!)

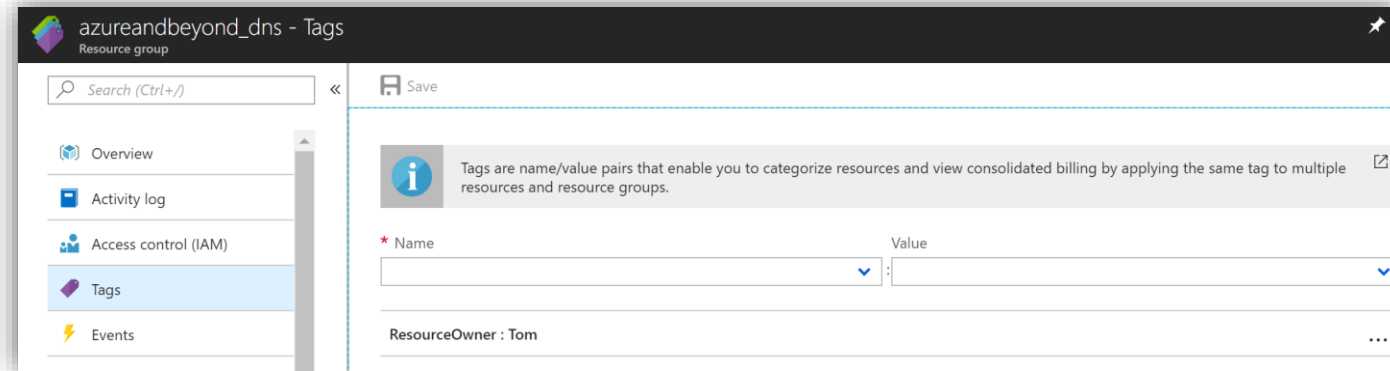


Resource Tags

Identifying Resources for Cost

Resource tags

- Name:Value → CostCenter:ProdIT, ResourceOwner:Tom
- Help to define responsibility and view consolidated billing
- Always tag RGs
 - Owner
 - Dept
 - CostCenter
- Tag resources as needed
- Define tags in advance



azureandbeyond_dns - Tags
Resource group

Search (Ctrl+/,)

Save

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups.

* Name Value

ResourceOwner : Tom

```
PS C:\> Get-AzureRmResource -TagName ResourceOwner -TagValue Tom | ft
```

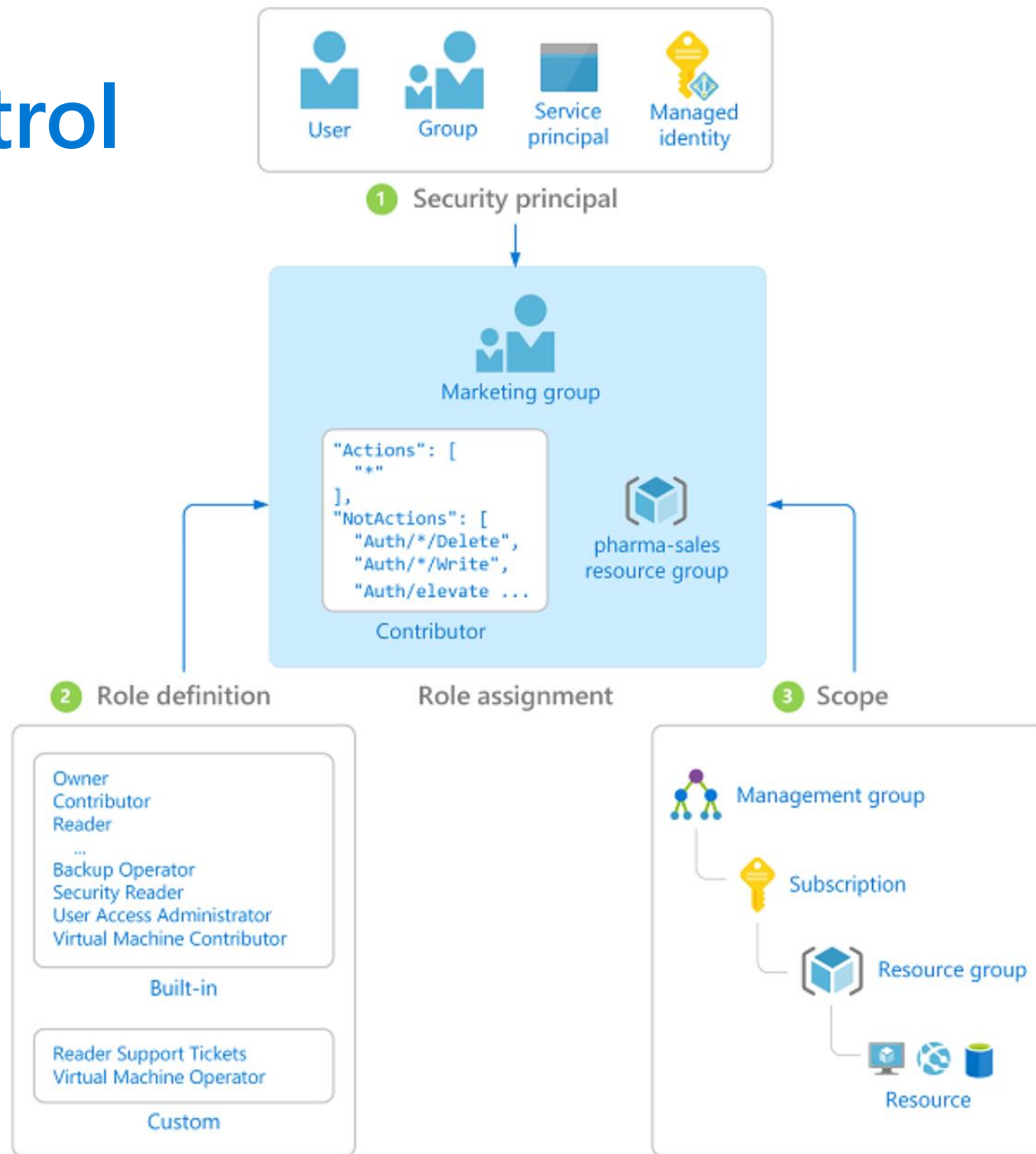
Name	ResourceGroupName	ResourceType	Location
azureandbeyond.eu	azureandbeyond_dns	Microsoft.Network/dnszones	global
lifecycletest	blobstorage-lifecyclemgmt	Microsoft.Storage/storageAccounts	westcentralus

Role Based Access Control

Using Identity to Manage Privilege

Role based access control

- Security principal
 - Object that represents a principal, or identity that is requesting access to Azure resources.
- Role definition
 - Collection of permissions listing operations that can be performed, such as read, write, and delete.
- Scope
 - Resources that the access applies to.
- Role assignments
 - Process of attaching a role definition to a principal or identity at a particular scope for the purpose of granting access.

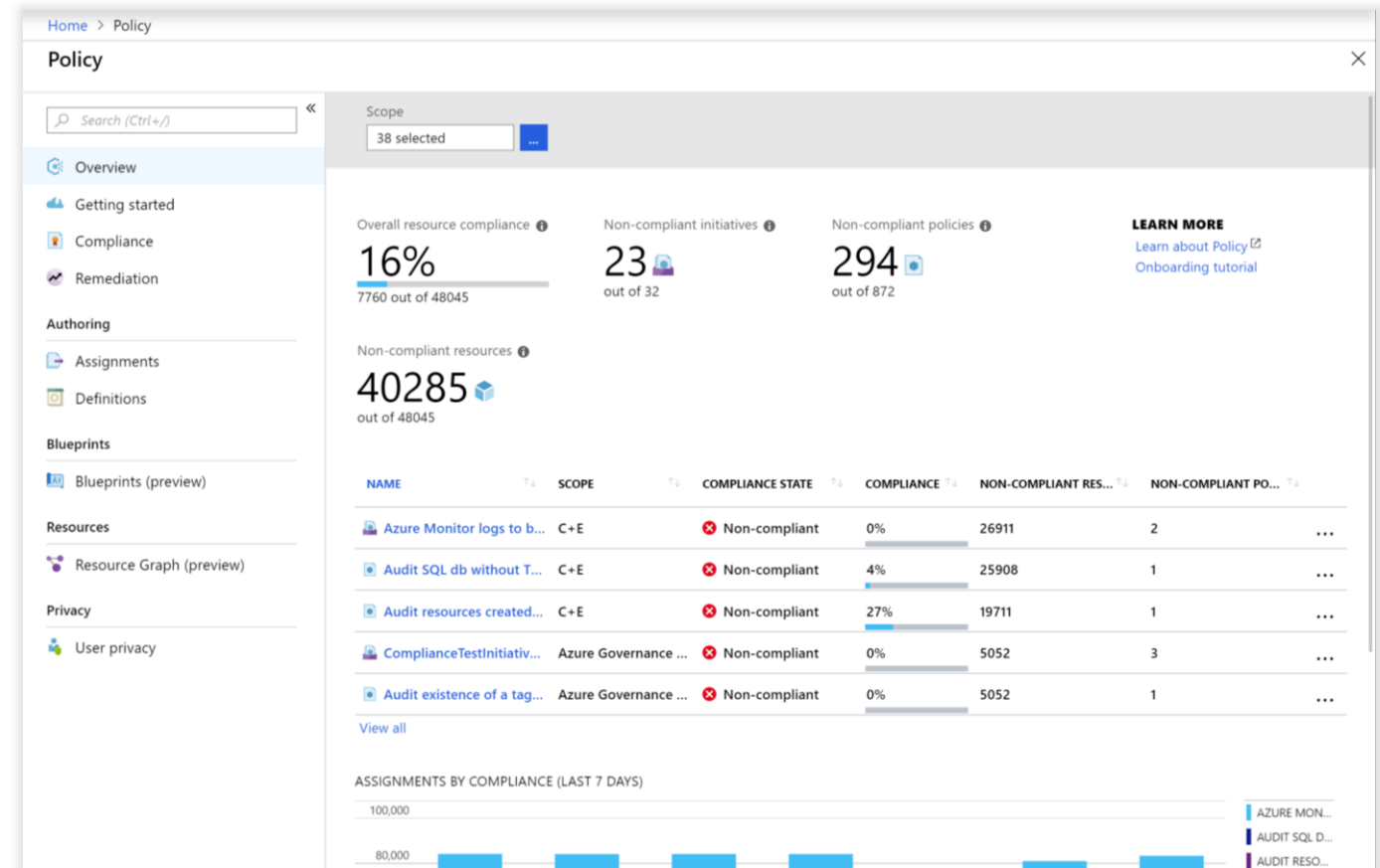


Policy

Real-time enforcement, compliance assessment, and remediation at scale.

Policy key info

- No other platform can do real time Policy enforcement
- No other cloud offers at-scale compliance assessment (and it's FREE for Azure!)
- Policy generate compliance events that can be used for alerting
- Aggregated and raw compliance data are available through API, Powershell & CLI
- Can be used to automatically remediate problems in your environment
- Policy evaluates all Azure resources & in-guest VM





Policy scenarios

- Restrict location or resource type (built-in)
- Inherit tags from Resource Group (see right ->)
- Block 'open to any' NSG rule creation ([Github](#))
- Enable diagnostic logs at-scale ([MVP blog](#))
- Security (built-in from Azure Security Center & In-Guest)

```
{
  "mode": "indexed",
  "policyRule": {
    "if": {
      "field": "tags.costCode",
      "exists": "false"
    },
    "then": {
      "effect": "append",
      "details": [
        {
          "field": "tags.costCode",
          "value": "[resourcegroup().tags.costCode]"
        }
      ]
    }
  }
}
```



Policy best practices

- Start with Audit Policies, which is a safe way of understanding what a policy will do without affecting user activity
- Used staged rollouts for Deny policies to understand impact
- Rollout remediation in stages

Details Definition (JSON)

 Duplicate this policy definition

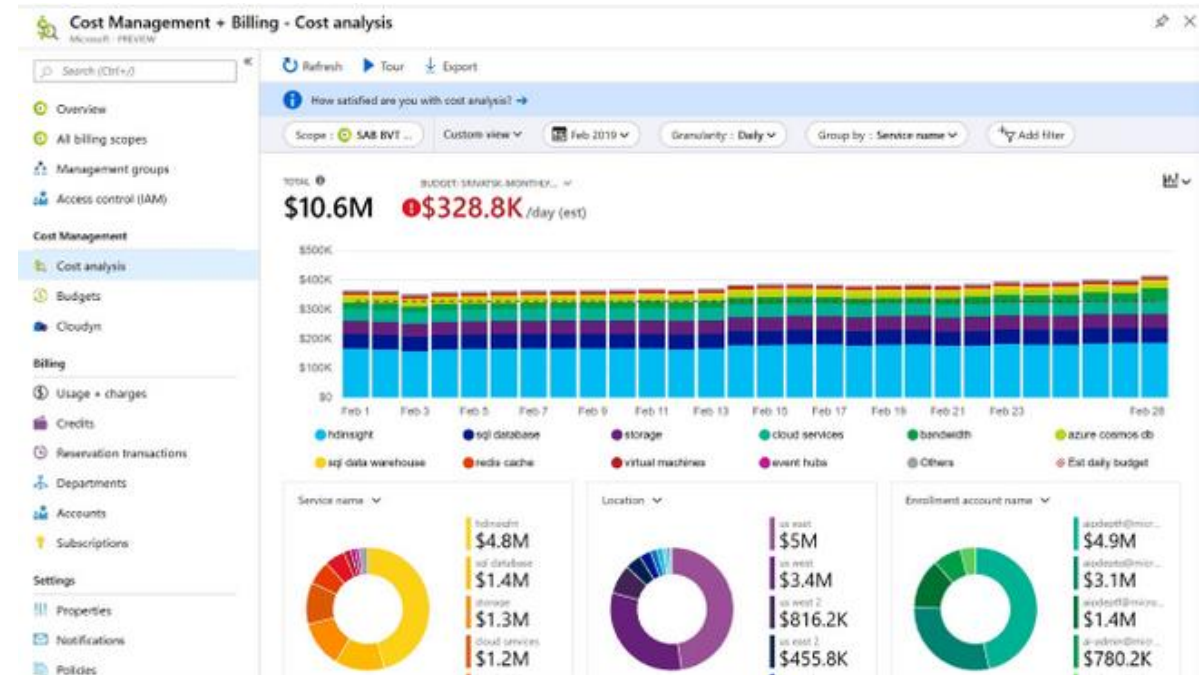
```
1 {
2   "if": {
3     "anyOf": [
4       {
5         "allOf": [
6           {
7             "field": "type",
8             "equals": "Microsoft.Compute/virtualMachines"
9           },
10          {
11            "field": "Microsoft.Compute/virtualMachines/osDisk.",
12            "exists": "True"
13          }
14        ]
15      },
16      {
17        "allOf": [
18          {
19            "field": "type",
20            "equals": "Microsoft.Compute/VirtualMachineScaleSet"
21          },
22          {
23            "anyOf": [
24              {
25                "field": "Microsoft.Compute/VirtualMachineScale",
26                "exists": "True"
27              },
28              {
29                "field": "Microsoft.Compute/VirtualMachineScale",
30                "exists": "True"
31              }
32            ]
33          }
34        ]
35      }
36    ],
37  },
38  "then": {
39    "effect": "audit"
40  }
41 }
```

Cost Management

Tracing the cash and setting the limits

Cost Control & budget's

- Monitor cloud spending
 - Track resource usage and manage costs across all your clouds with a single, unified view, and access rich operational and financial insights to make informed decisions.
- Increase organizational accountability
 - Implement governance policies for effective enterprise cloud cost management, and increase accountability with budgets, cost allocation, and chargebacks.
- Optimize cloud efficiency
 - Improve the return on your cloud investment by using continuous cost optimization and industry best practices.



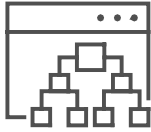
Azure Blueprints

Deploy and update cloud environments in a repeatable manner using composable artifacts



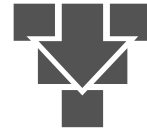
Azure Blueprints

Use Cases



Manage Environments

Idempotent definition
to safely and
efficiently provision
and manage infra at
scale



Reduce Complexity

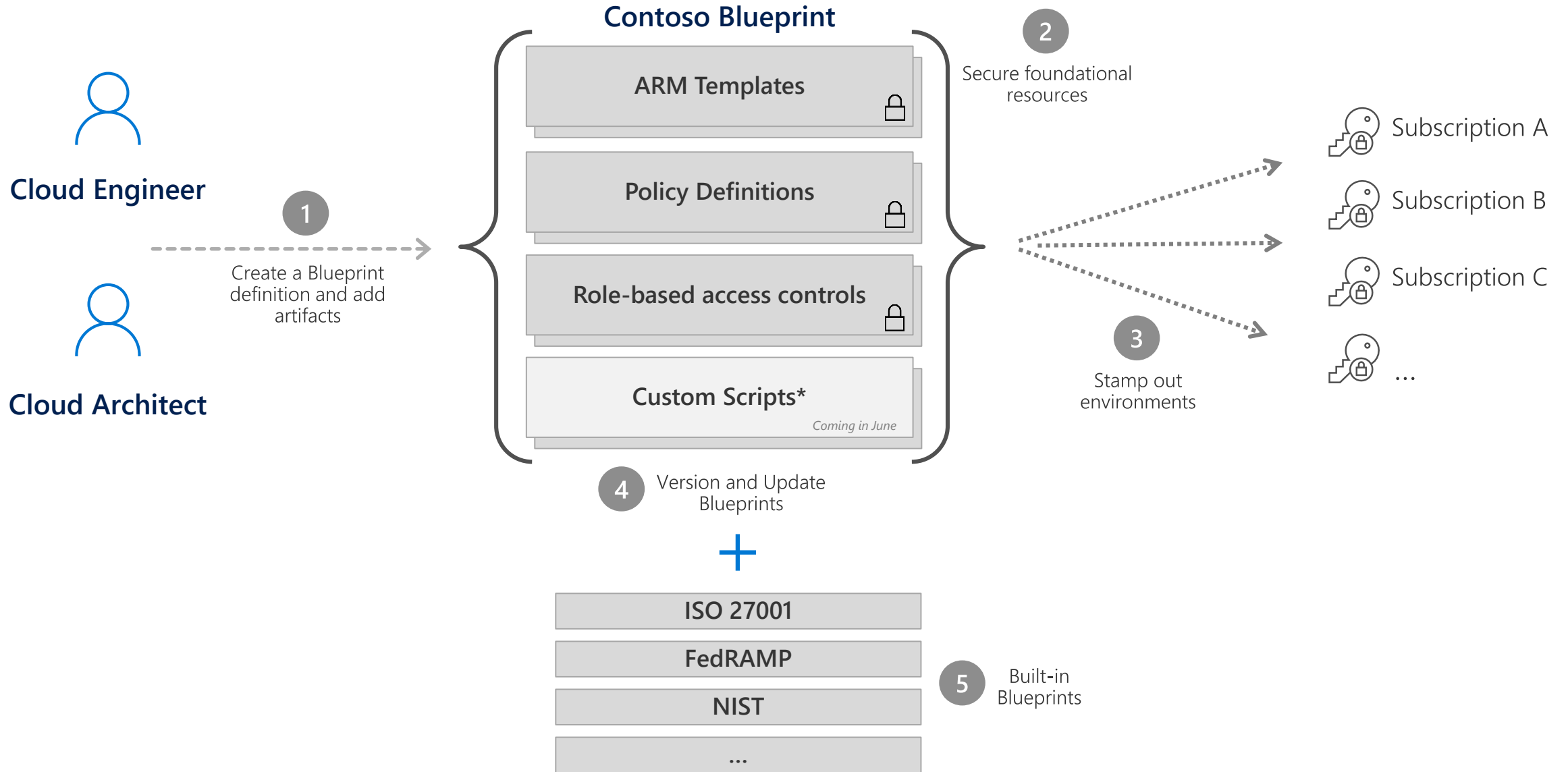
Define all your
artifacts (policies,
RBAC and templates)
that go into an
environment in
simple experience



Secure Resources

Lock down
foundational infra
that are shared
across subscriptions

How it works



Common Sense

Grouping of subscriptions and managing hierarchy



... is not so common!

- *Voltaire*