

Empower your Governance with Azure Policy

by Gregor Reimling



Cologne

Virtual





Gregor Reimling



Cloud Consultant @Sepago



Cloud and Datacenter, Governance



Azure Infrastructure (Governance, IaaS, Security)



info@reimling.eu



@GregorReimling | @AzureBonn



www.reimling.eu | www.neutralien.com

Identity Summit 2020
follow








@IdentitySummit



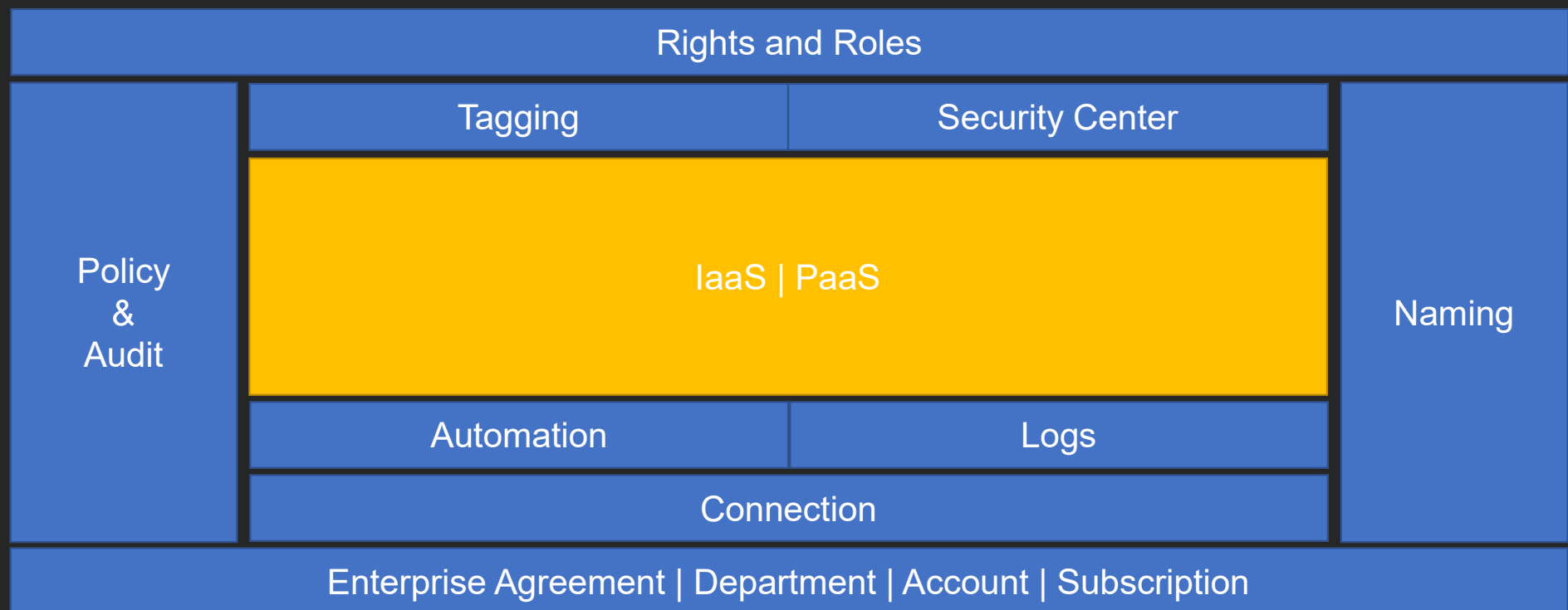
www.AzureBonn.de

Agenda

- Governance Overview
- Architecture
- How does it work
- Demo
- VM Guest Policy

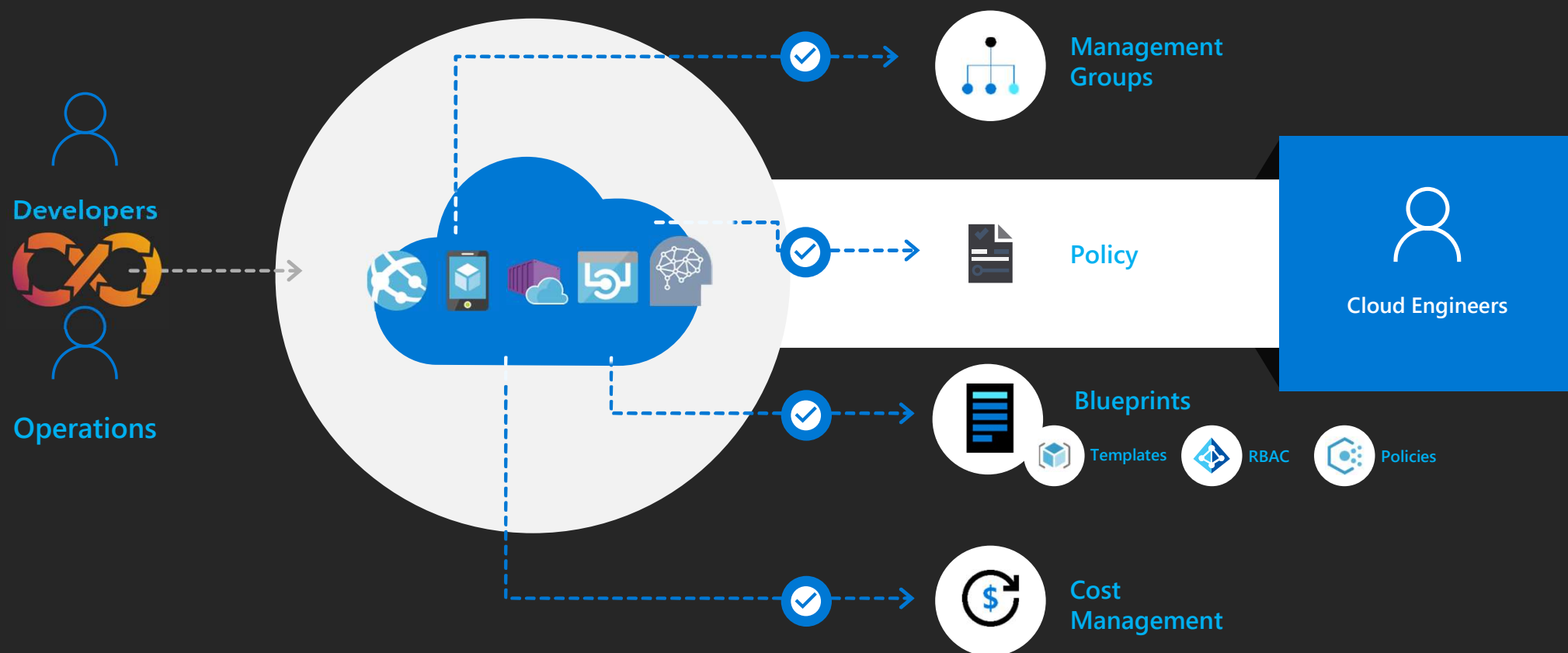
				
Governance <small>NEW</small>	Security	Resiliency	Monitoring	Automate
Proactively apply policies and optimize cloud spend	Industry leading Security with Advanced Threat Protection	High availability and protection for VMs, apps and data	Deep operational insights with rich intelligence	Powerful scripting, configuration and update management

Azure Governance



Speed + Control

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

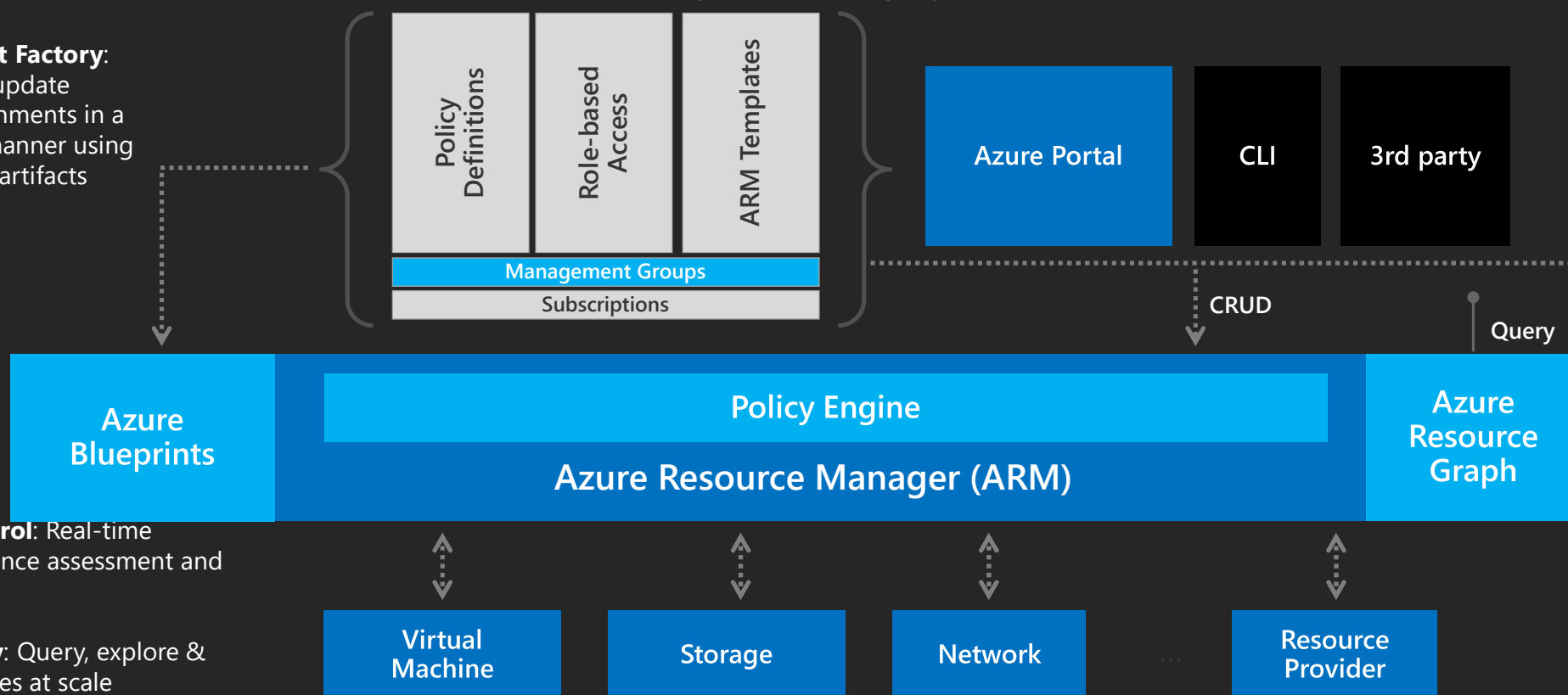


Azure Governance Architecture

providing control over the cloud environment, without sacrificing developer agility

1. Environment Factory:

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



2. Policy-based Control: Real-time enforcement, compliance assessment and remediation at scale

3. Resource Visibility: Query, explore & analyze cloud resources at scale

Azure Policy

- Create, assign and manage policies
- Enforce rules to ensure your resources are compliant
- Focus on resource properties for new and existing deployments

Azure Policy Concepts

- A definition is a rule
- An assignment is an application for an initiative or a policy of a specific scope
- An initiative is a group of policies

Leverage built-in initiative & policies



Security

Azure Security Center
Guest Config baselines
Key Vault certificate
NSG rules
AKS & AKS Engine
RBAC role assignment



Regulatory Compliance

NIST SP 800-53 R4
ISO 27001:2013
CIS
PCI v3.2.1:2018
FedRAMP Moderate
Canada Federal PBMM
SWIFT CSP-CSCF v2020
UK Official and UK NHS
IRS 1075



Tags

Require specified tag
Add or replace a tag
Inherit a tag from the RG
Append a tag



Resource standardization

Allowed/ not allowed RP
Allowed locations
Naming convention
Back up VMs
Allowed images for AKS



Cost

Allowed VM SKUs
Allowed Storage SKUs

Azure Policy



- Turn on built-in policies or build custom ones for all resource types
- Real-time policy evaluation and enforcement
- Periodic & on-demand compliance evaluation
- VM In-Guest Policy (NEW)

Enforcement & Compliance



- Apply policies to a Management Group with control across your entire organization
- Apply multiple policies and & aggregate policy states with policy initiative
- Exclusion Scope

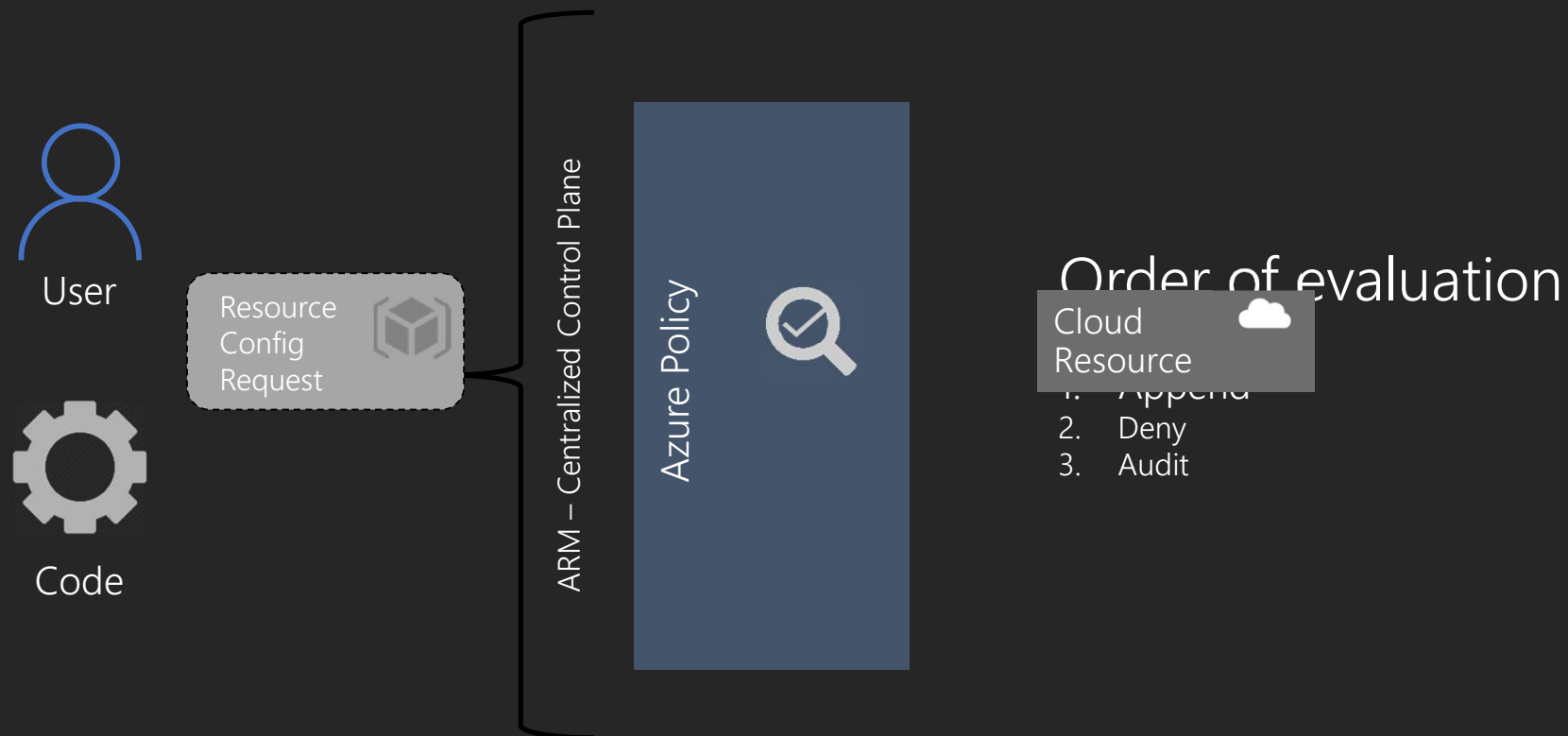
Apply policies at scale



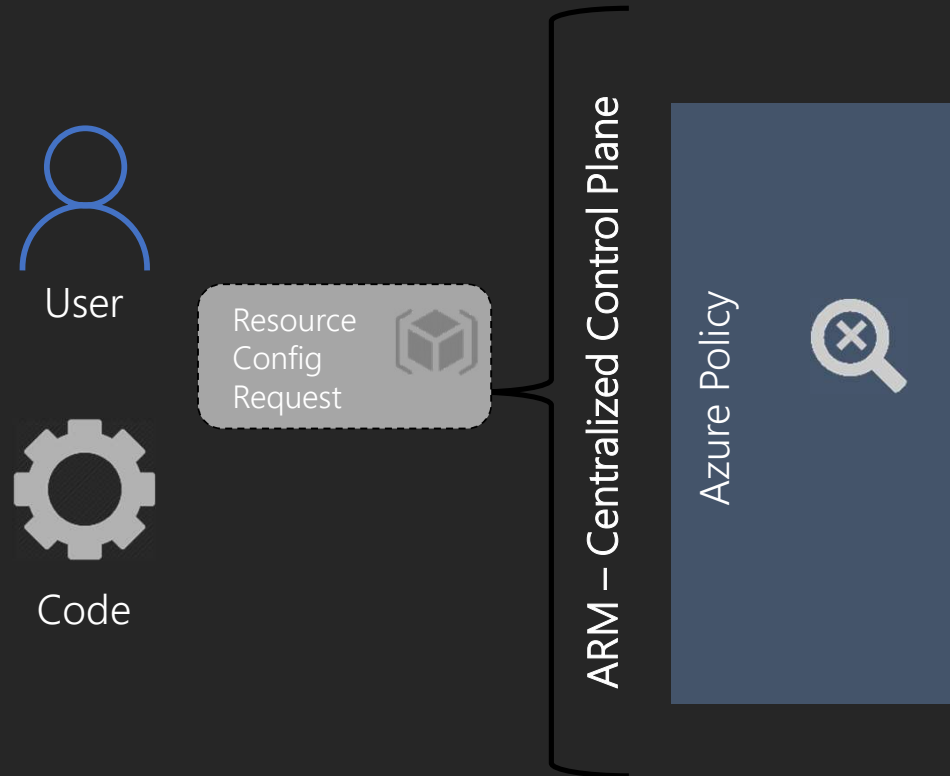
- Real time remediation
- Remediation on existing resources (NEW)

Remediation

How does it work?



How does it work?



How does it work?



User



Code

ARM – Centralized Control Plane

Azure Policy



Cloud
Resource



4. DeployIfNotExists
5. AuditIfNotExists

Order of evaluation

- Append
- Deny
- Audit
- DeployIfNotExists
- AuditIfNotExists

Azure Policy Definition structure

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

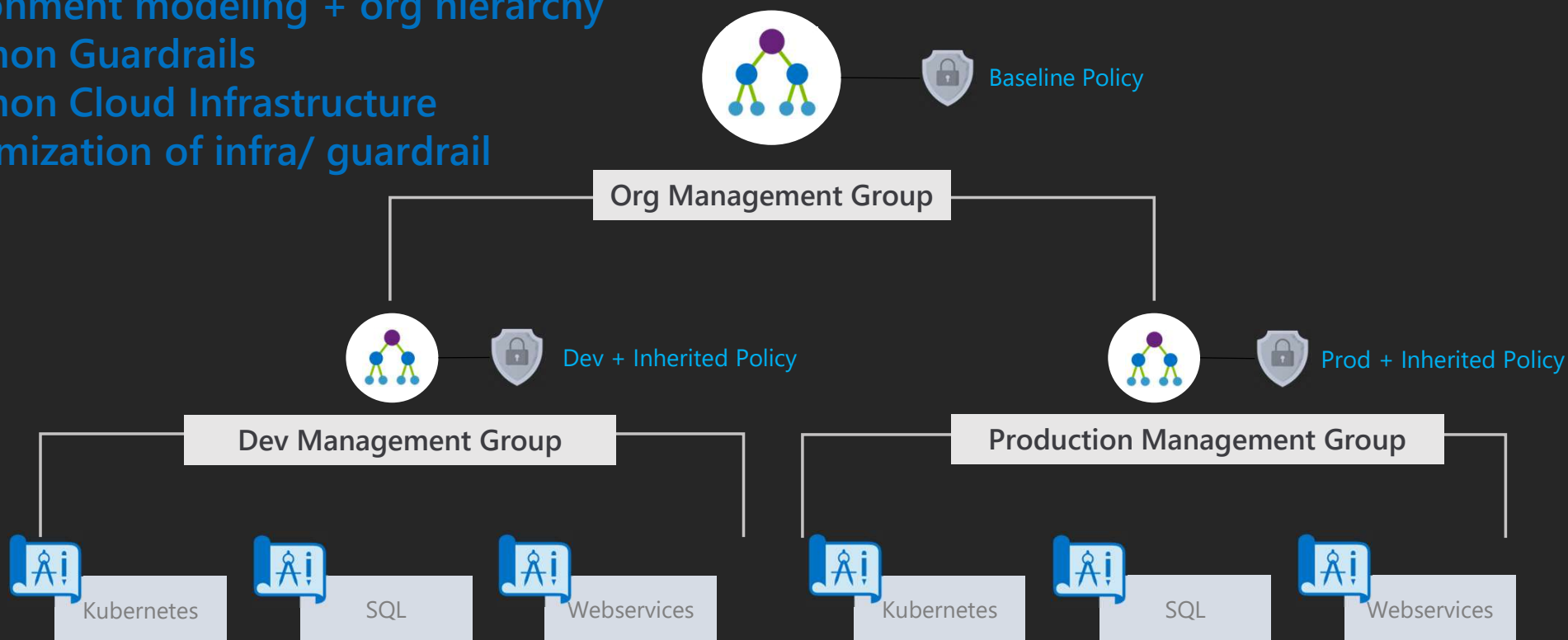
Azure Policy

DEMO

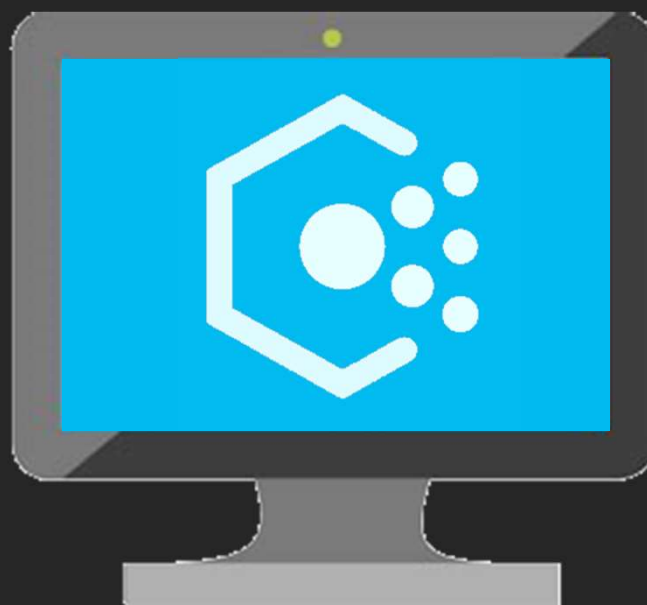


Management Groups

Environment modeling + org hierarchy
Common Guardrails
Common Cloud Infrastructure
Customization of infra/ guardrail



Introducing VM guest policy



Guest Config Policy

Policy that audit settings within the VM's guest environment

Azure Policy for In-Guest VM Config [preview]

DSC v.2 (Windows) and Chef InSpec (Linux)

Configuration of the operating system

Application configuration or presence

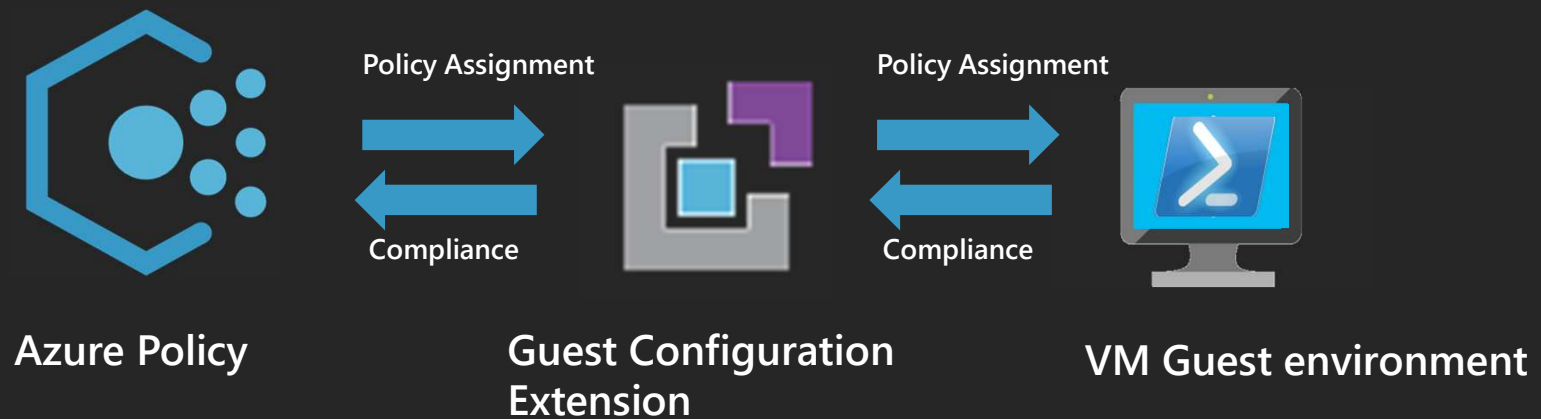
Environment settings

Join preview: <https://aka.ms/inguestpolicy>



NAME	DEFINITION LOCATION
Audit Windows VMs in which the Administrators group does not contain only the specified members	
[Preview]: Audit Windows VMs on which the Log Analytics agent is not connected as expected	
Audit Windows VMs in which the Administrators group does not contain all of the specified members	
Audit Windows VMs that do not have the specified applications installed	
[Preview]: Audit VMs with insecure password security settings	
Audit Windows VMs that are not set to the specified time zone	
Audit Windows VMs that are not joined to the specified domain	
Audit Windows web servers that are not using secure communication protocols	
Audit Windows VMs on which the specified services are not installed and 'Running'	
[Preview]: Audit Windows VMs on which Windows Defender Exploit Guard is not enabled	
Audit Windows Server VMs on which Windows Serial Console is not enabled	
Audit Windows VMs in which the Administrators group contains any of the specified members	
[Preview]: Audit Windows VMs that contain certificates expiring within the specified number of days	
[Preview]: Audit Windows VMs that have not restarted within the specified number of days	
[Preview]: Audit Windows VMs on which the DSC configuration is not compliant	
Audit Linux VMs that do not have the specified applications installed	
Audit Windows VMs with a pending reboot	
Audit Windows VMs that do not have the specified Windows PowerShell modules installed	
[Preview]: Audit Windows VMs that do not contain the specified certificates in Trusted Root	
Audit Windows VMs that have the specified applications installed	
Audit Linux VMs that have the specified applications installed	

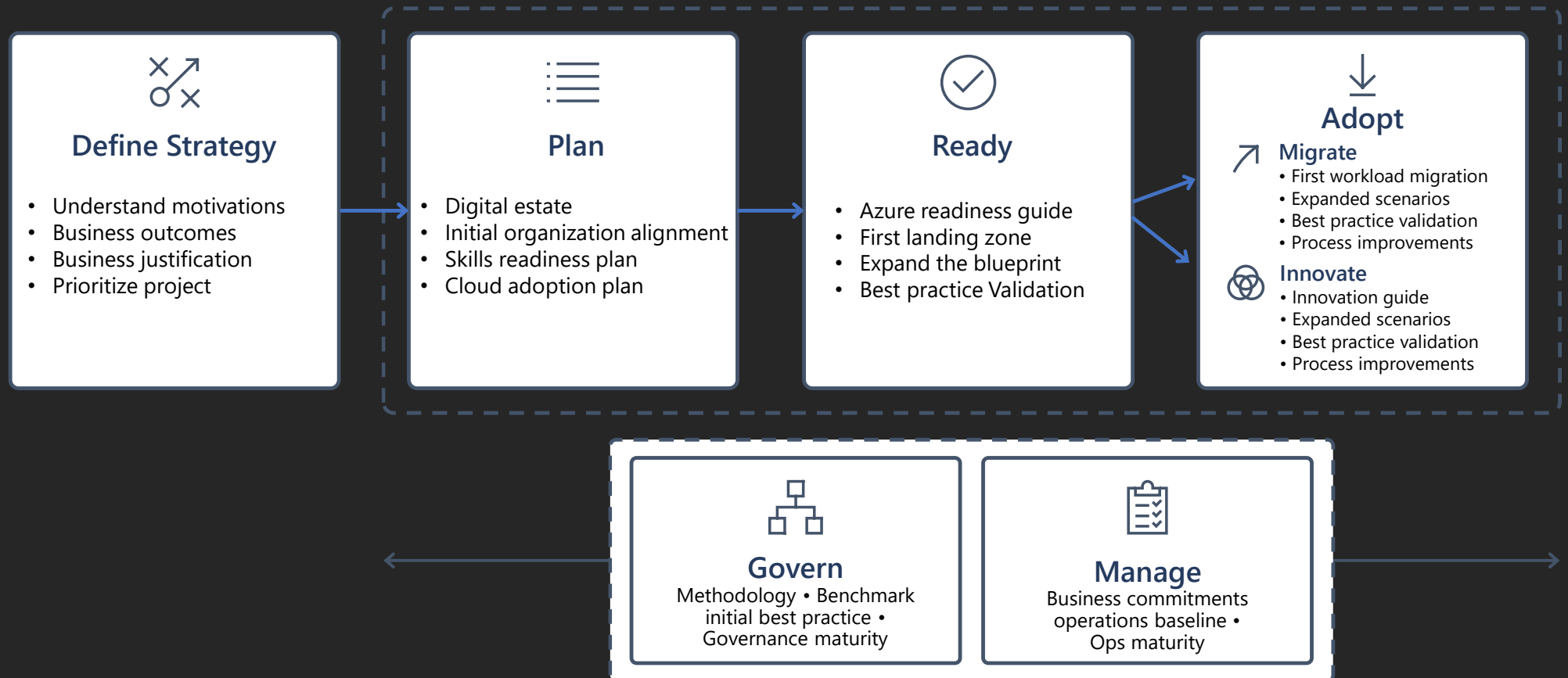
How VM guest policy works



Policy

- 250 policy definitions per scope
- 100 policy set definitions per scope
- 1000 policy set definitions per tenant
- 100 policyDefinition references per policySetDefinition
- 100 policy assignments per scope
- 250 notScopes per policyAssignment
- <https://github.com/Azure/azure-policy>

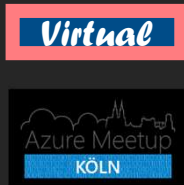
Microsoft Cloud Adoption Framework for Azure



Links

- <https://docs.microsoft.com/en-us/azure/governance/policy/overview>
- <https://docs.microsoft.com/en-us/azure/governance/policy/>
- <https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage>
- <https://www.reimling.eu/2019/03/azure-management-groups-und-blueprints-ueberblick-und-einrichtung-teil-1/>
- <https://github.com/Azure/azure-policy/>

Thanks to the sponsors and the Azure CGN Team





pmOne



Questions? ->
Reach me via Twitter 😊

Identity Summit 2020
follow

 @IdentitySummit

 @GregorReimling | @AzureBonn
 www.reimling.eu | www.azurebonn.de

