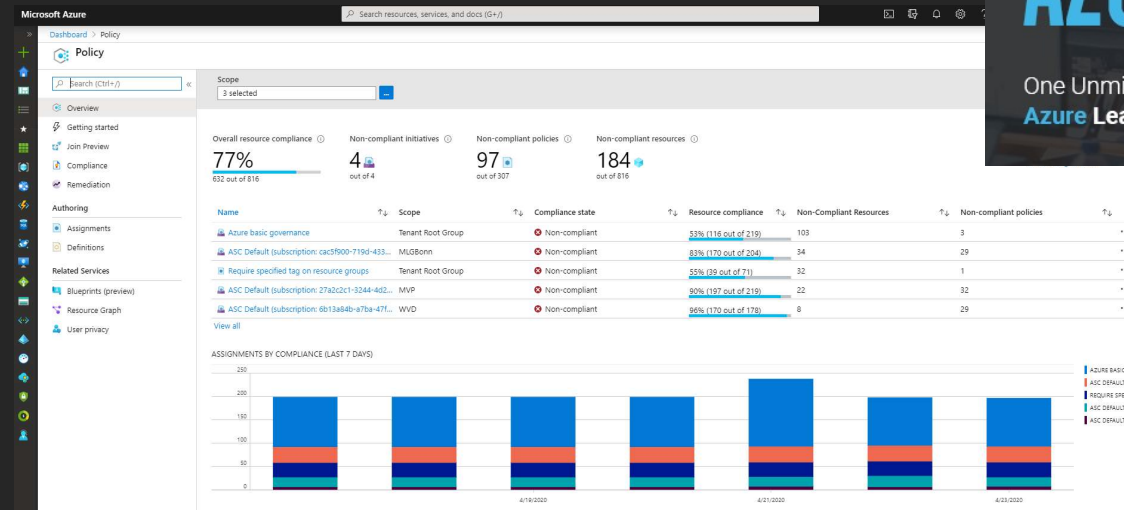


# AZURE WEEK

25 - 29  
MAY

One Unmissable Week of Free Online  
**Azure Learning**

**SIGN ME UP**



# Azure Policy with Azure Security Center - Your Cloud Guards

by Gregor Reimling

Please go to [menti.com](https://menti.com) and enter [47 03 81](https://menti.com/join/470381)



# Gregor Reimling



Cloud Consultant @Sepago



Cloud and Datacenter, Governance



Azure Infrastructure (Governance, IaaS, Security)



[info@reimling.eu](mailto:info@reimling.eu)



[@GregorReimling](https://twitter.com/GregorReimling) | [@AzureBonn](https://twitter.com/AzureBonn)



[www.reimling.eu](http://www.reimling.eu) | [www.neutralien.com](http://www.neutralien.com)

Identity Summit 2020  
follow



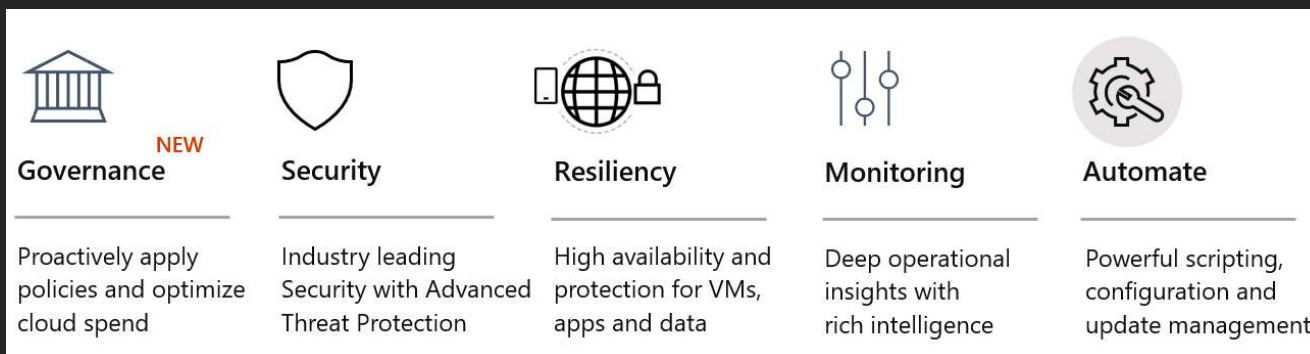
[@IdentitySummit](https://twitter.com/IdentitySummit)



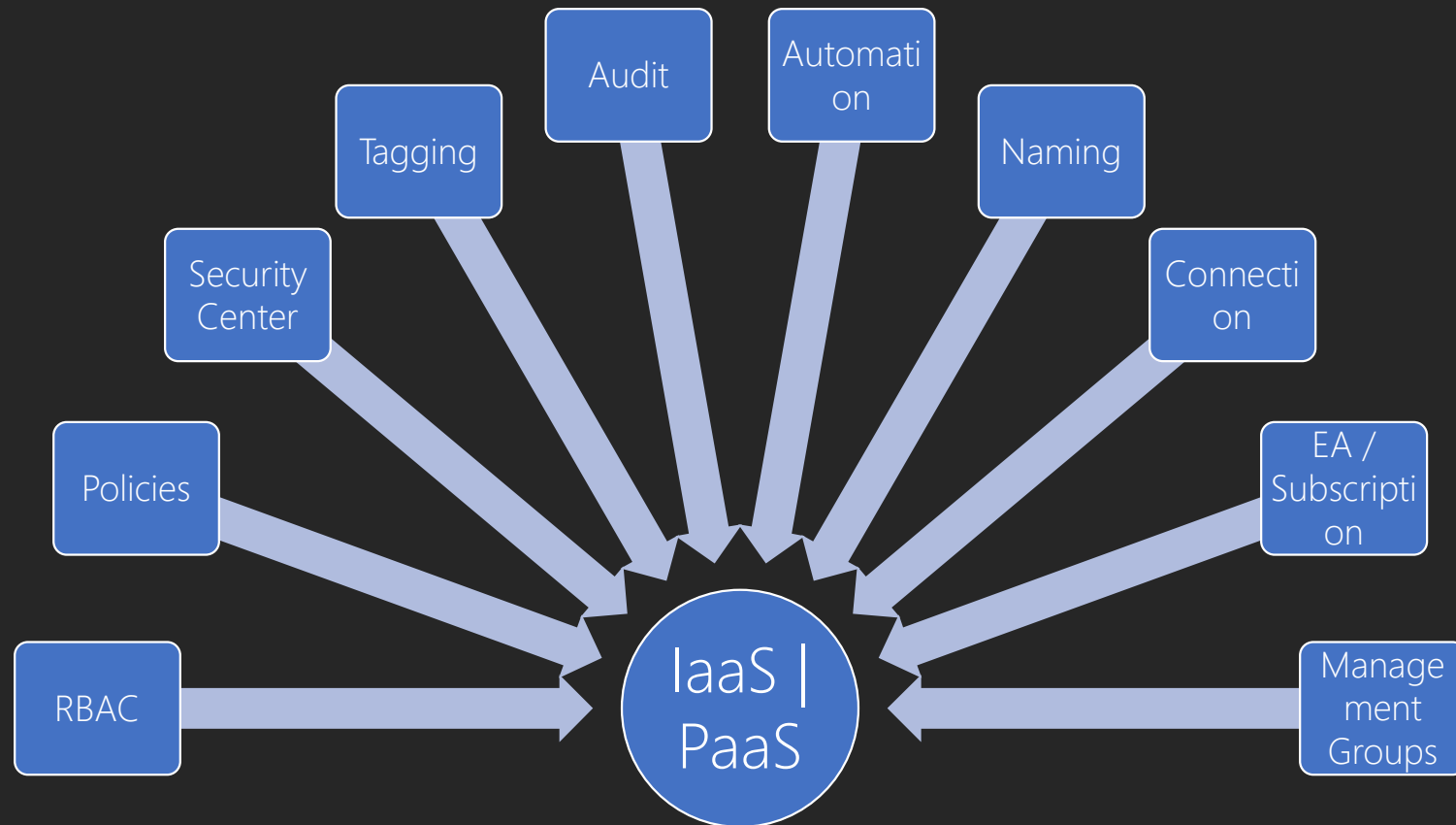
[www.AzureBonn.de](http://www.AzureBonn.de)

# Agenda

- Azure Policy
- Azure Security Center
- How does it work together
- Summary

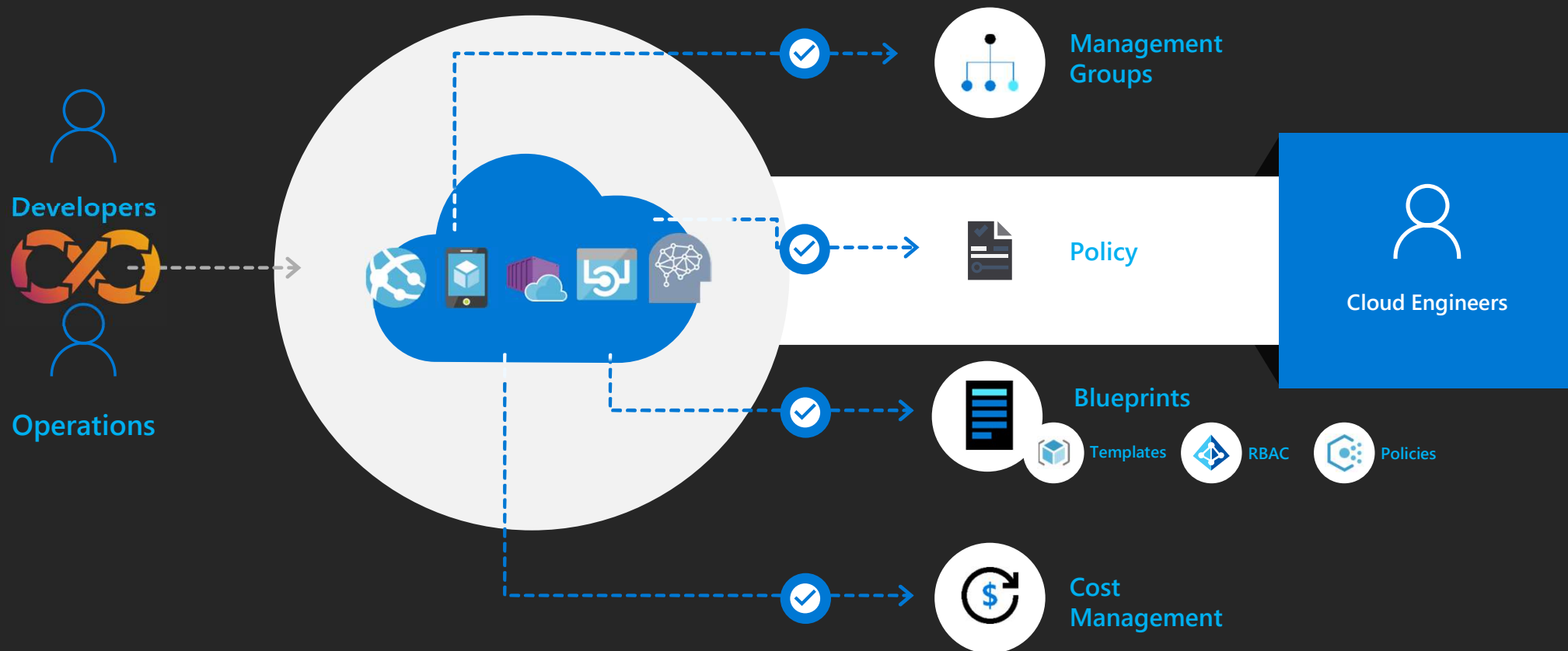


# Azure Governance



# Speed + Control

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



# Azure Policy Concepts

- Create, assign and manage policies
- Enforce rules to ensure your resources are compliant
- Focus on resource properties for new and existing deployments
- A definition is a set of conditions in audit or deny mode
- An assignment is a policy definition placed on a specific scope
- An initiative is a collection of policies

# 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)

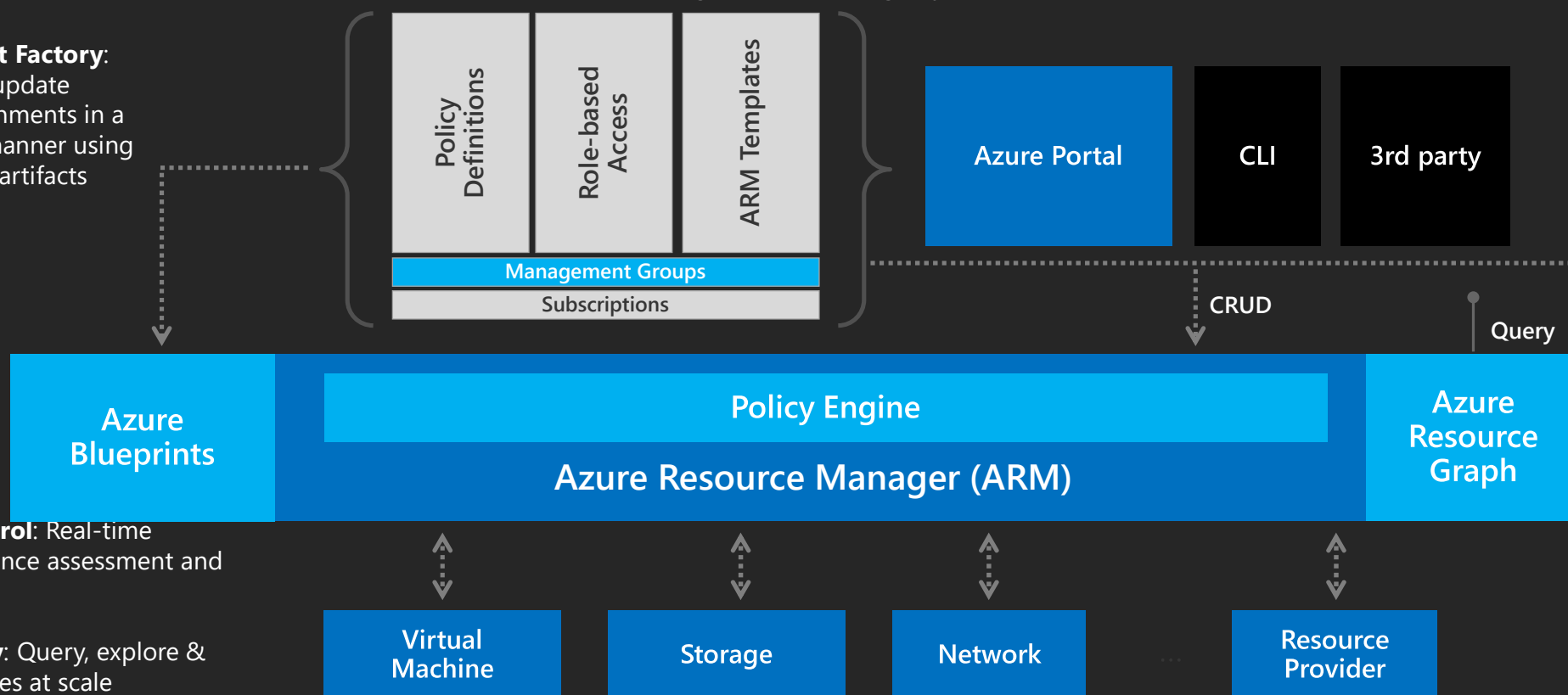
## Remediation

# 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



# 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

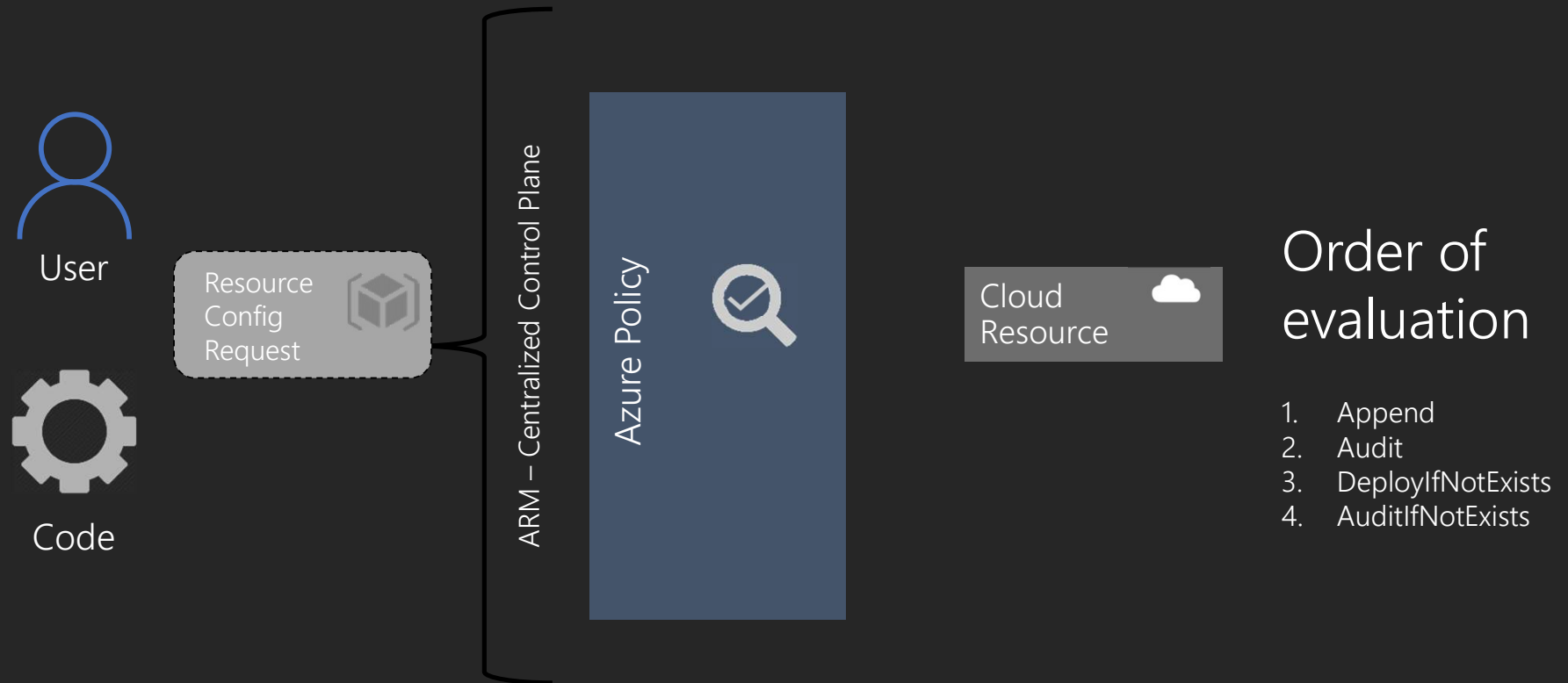
Allowed VM SKUs  
Allowed Storage SKUs

# Azure Policy

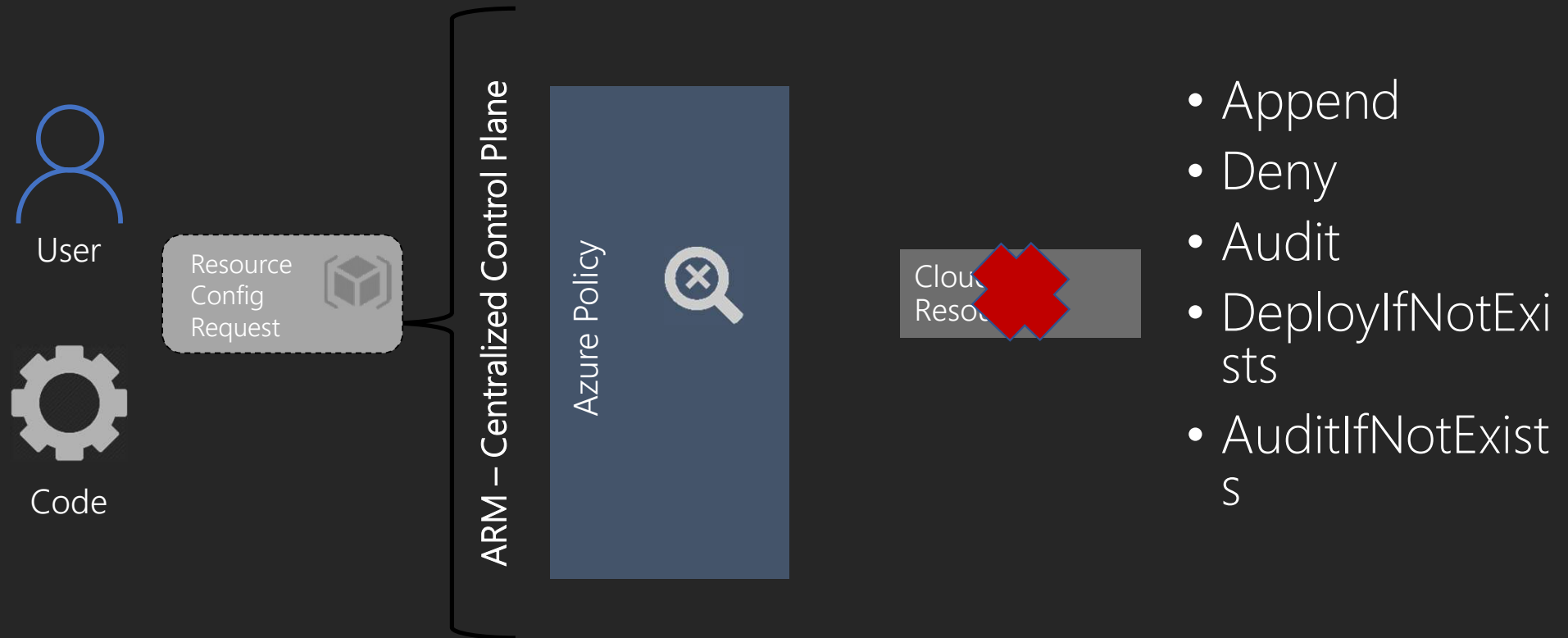


**DEMO**

# How does it work?



## How does it work?



# Azure Policy



**DEMO**

# 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"  
      } } } }
```

# 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>

# Azure Security Center





# Azure Security Center

- A service to strengthen your security posture
- Available in two Tiers – Basic and Standard
- Basic -> Free – Activated by default for all subscriptions
- Based on an security score – scope based
- Available for all workloads (Server, Container, SQL, IoT and more)

# Azure security center



## Strengthen security posture

### Cloud security posture management

Secure Score  
Policies and compliance



## Protect against threats

For  
servers

For cloud native  
workloads

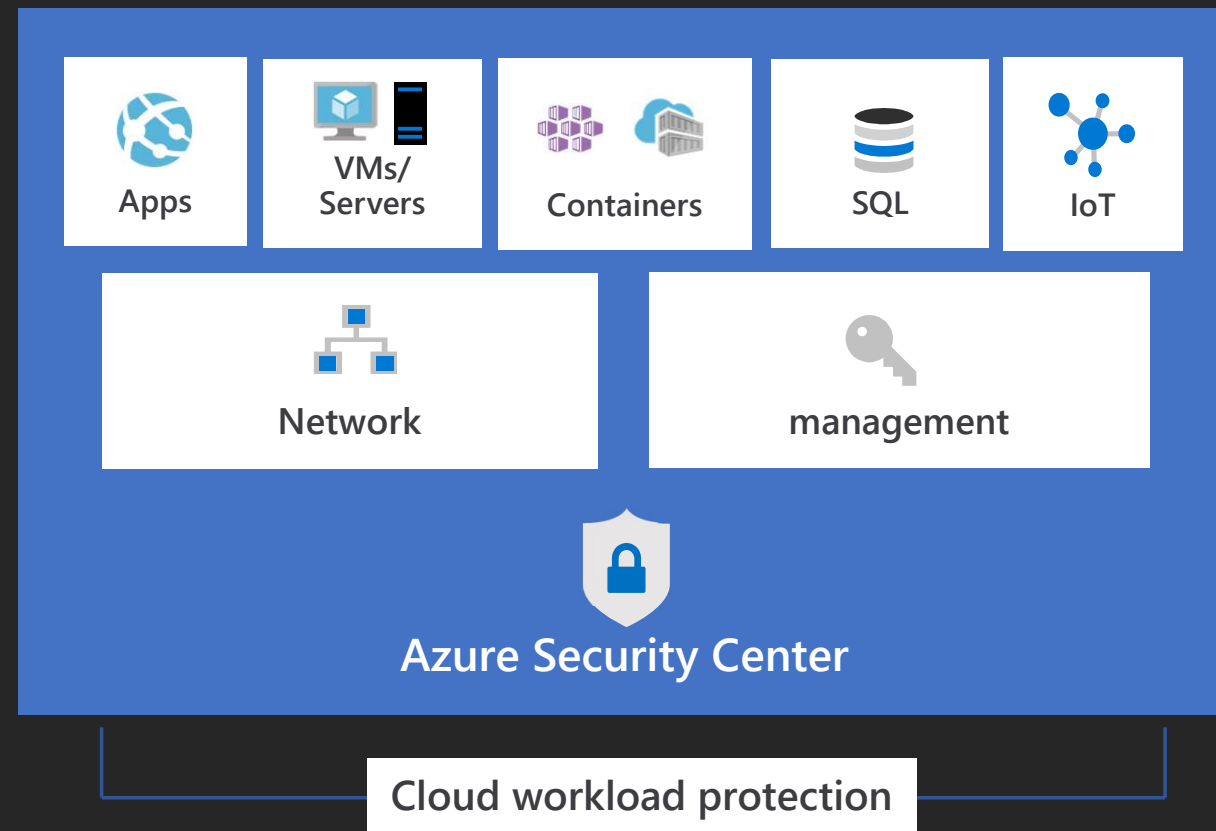
For  
databases  
and storage



Get secure faster

## Protect your workloads

- Detect & block advanced malware and threats for Linux and Windows Servers on any cloud
- Protect cloud-native services from threats
- Protect data services against malicious attacks
- Protect your Azure IoT solutions with near real time monitoring
- Service layer detections: Azure network layer and Azure management layer (ARM)



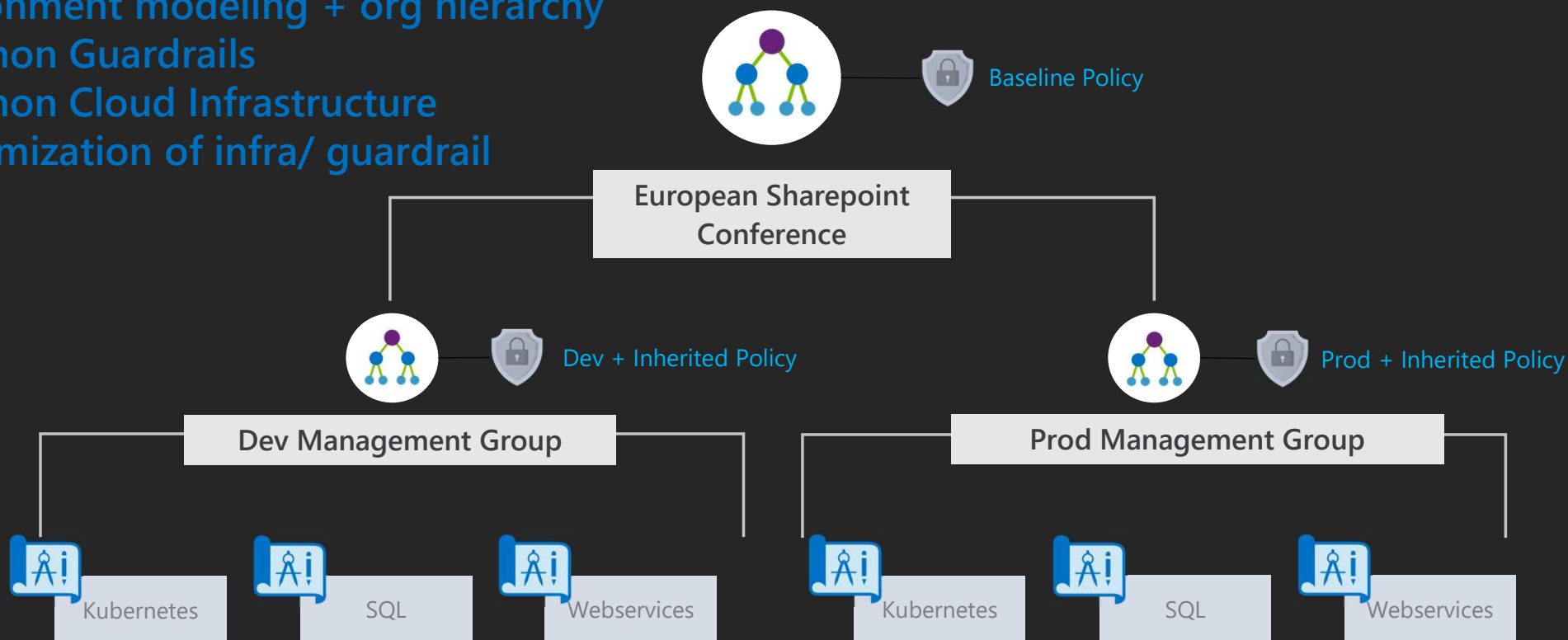
# Azure Security Center



**DEMO**

# Management Groups

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



## How it works together

- All Azure Security Center recommendations based on Azure Policy
- Secure score is result of Azure Policy settings
- Recommendation is also a result of Azure Policy
- All Azure Policy are defined in Compliance mode

# Using custom security polices in ASC

- You can define custom security policies for Secure score
- Use Management Group for scoping
- Own security policies will display as custom
- Enhanced information for recommendation is possible
  - Needs to define additional settings in the definition

JSON

Copy

```
"metadata": {  
  "securityCenter": {  
    "RemediationDescription": "Custom description goes here",  
    "Severity": "High",  
  },  
}
```

# Azure Security Center



**DEMO**



## Azure Policy Recap

- Powerful solution to define Cloud Guards for own Tenant
- Start with an audit effect instead of a deny effect
- Define Management Groups to group subscriptions and set Policies at Higher level
- Use Deny effect for Production workloads with wisdom
- Creating initiatives even for single policy definition
- Integrate Azure Policy in your regular Azure check

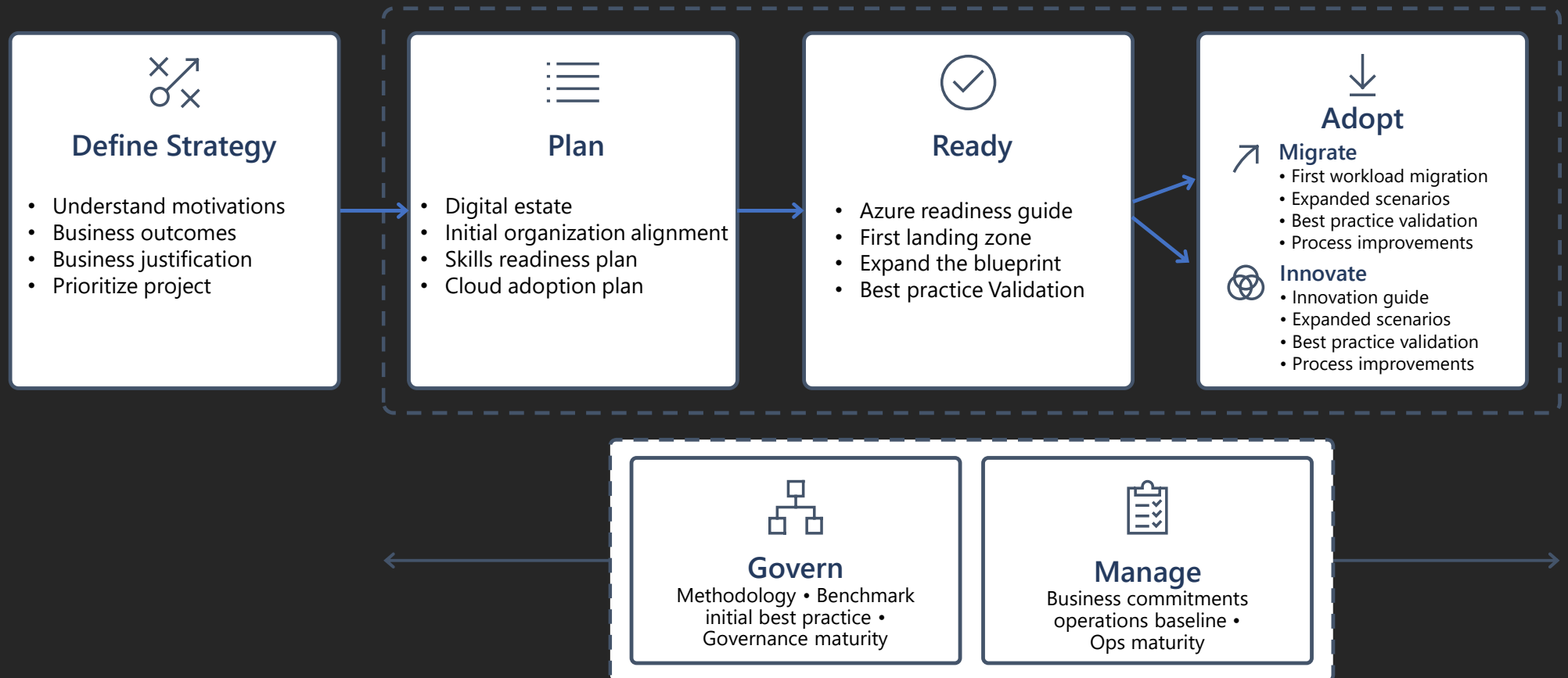
# Azure Security Center

- Start with ASC to get a Security Overview
- Use ASC to strengthen your infrastructure
- Check the status in ASC regularly
- Create own security policies for secure score
- Use ASC to proof your infrastructure
- Integrate Azure Policy in your regular Azure check

# 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/>
- <https://aka.ms/SecurityCommunity>
- <https://docs.microsoft.com/en-us/azure/security-center/>
- <https://docs.microsoft.com/en-us/azure/security-center/security-center-policy-definitions>
- <https://docs.microsoft.com/en-us/azure/security-center/custom-security-policies>
- <https://blog.azureandbeyond.com/2020/04/24/mastering-azure-security-my-latest-adventure/>



# Microsoft Cloud Adoption Framework for Azure



Questions? ->  
Reach me via Twitter 😊

Identity Summit 2020  
follow

 @IdentitySummit

 @GregorReimling | @AzureBonn  
 [www.reimling.eu](http://www.reimling.eu) | [www.azurebonn.de](http://www.azurebonn.de)