Gregor Reimling

# Azure Policy with ASC

Kilbirnie – 12:00

#ScottishSummit2021

# Our Sponsors

ScriptRunner®
The #1 for PowerShell Management

DQ GLOBAL
DRIVING **DATA** QUALITY

PROXIMO3
MICROSOFT CONSULTING SPECIALISTS

Redspire

Agilisys

Hitachi Solutions

# Gregor Reimling

MS Azure MVP

Founder of AzureBonn

@GregorReimling

www.reimling.eu

# Agenda

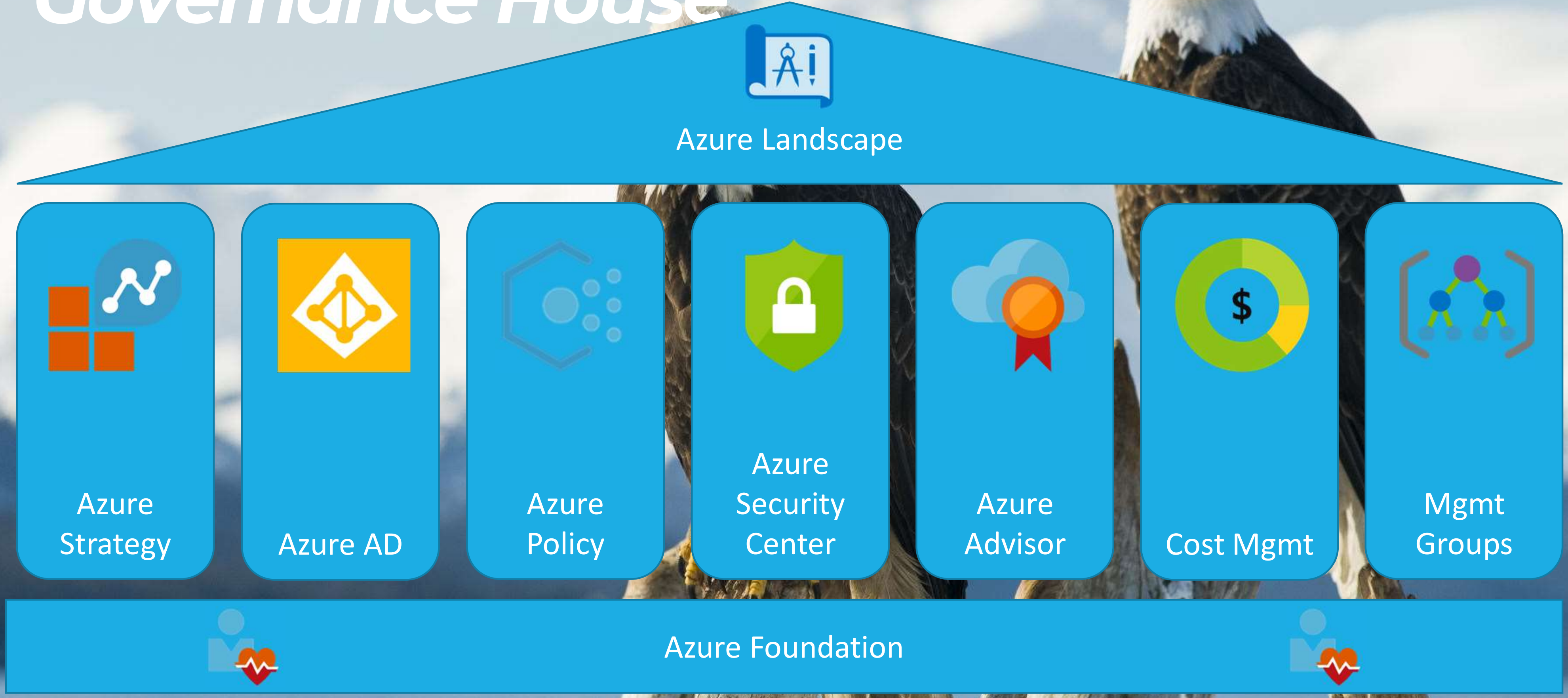
Azure Policy

Azure Security Center

How does it work together

Summary

# Azure Governance House



Azure Landscape

Azure Strategy

Azure AD

Azure Policy

Azure Security Center

Azure Advisor

Cost Mgmt

Mgmt Groups

Azure Foundation

Scottish Summit Template

# Azure Policy

## Enforcement & Compliance

- 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**)

## Apply policies at scale

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

## Remediation

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

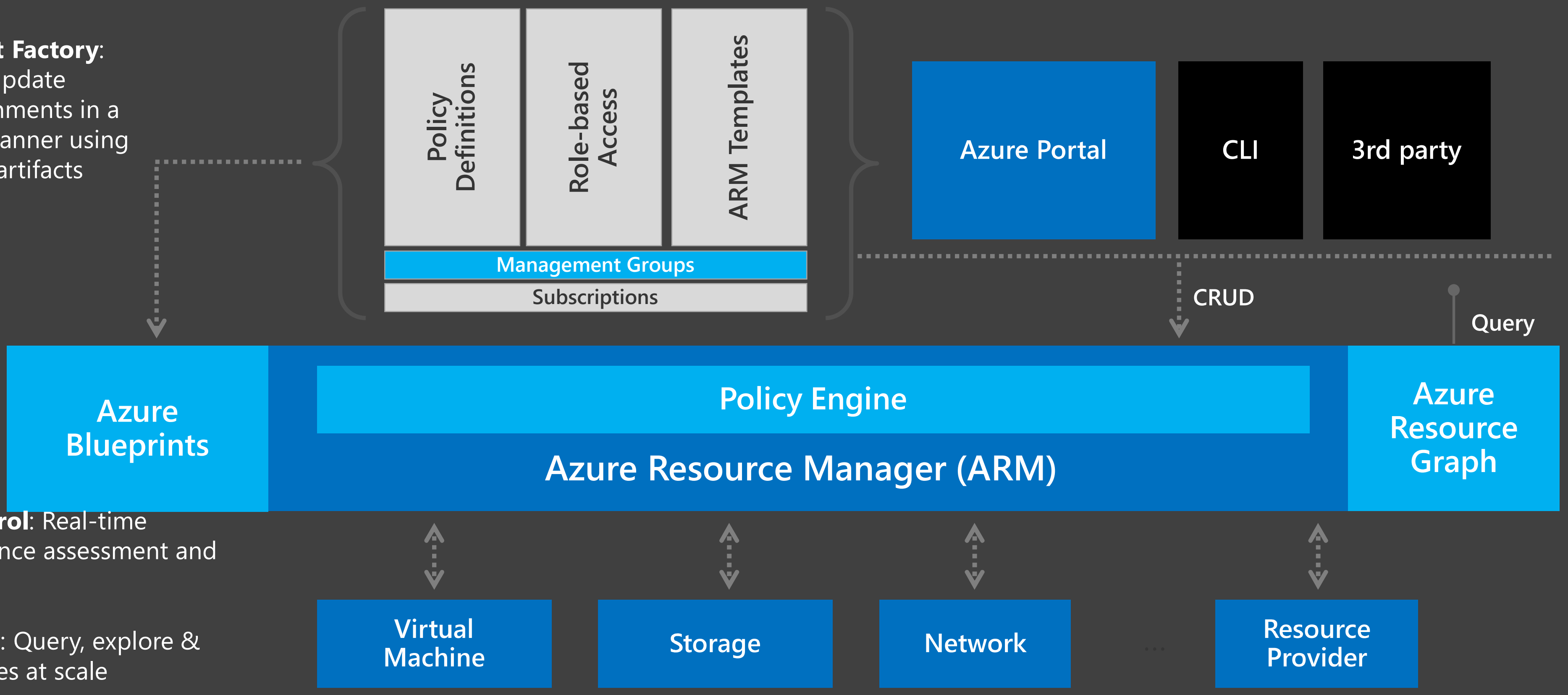
# Azure Policy

- Create, assign and manage policies
- Enforce rules to ensure your ressoures are compliant
- Focus on ressource 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 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

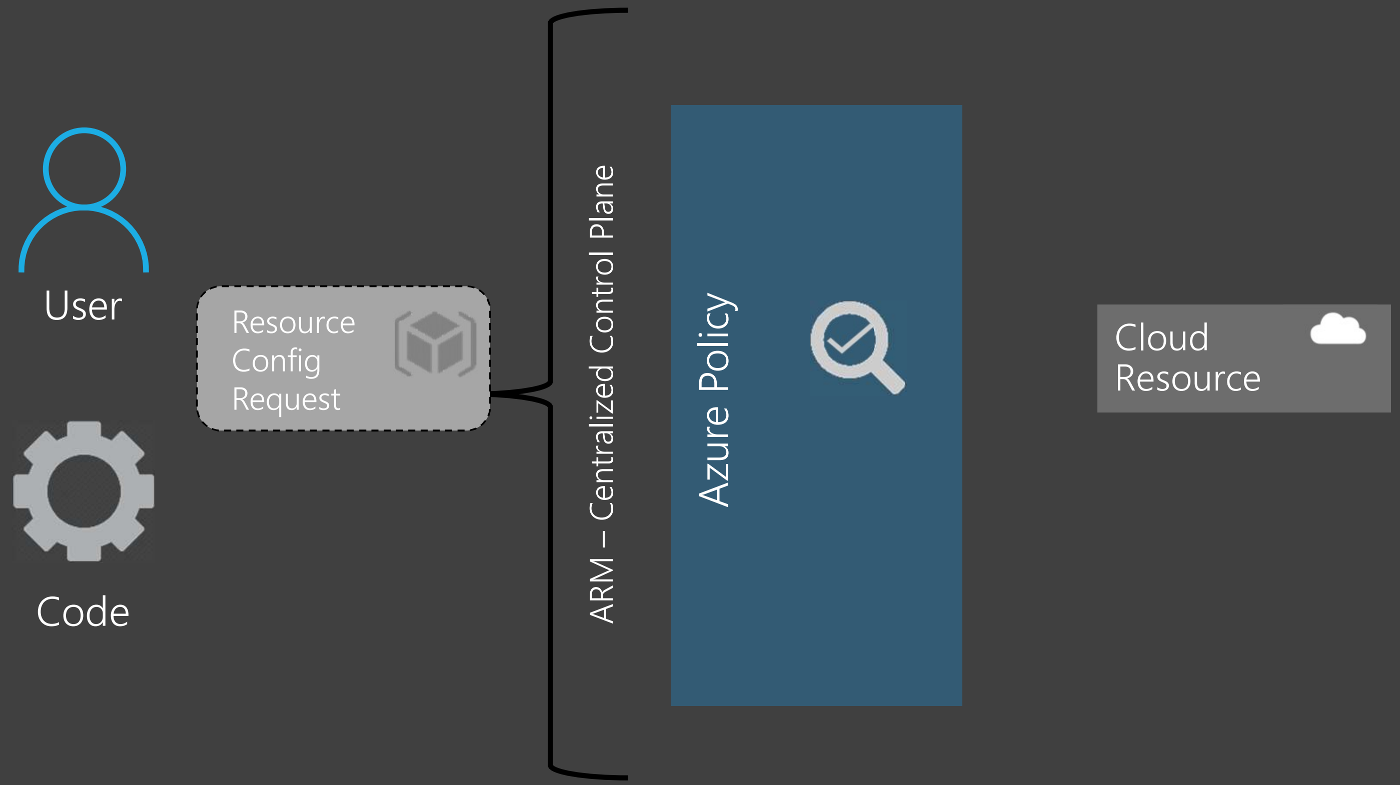
Allowed images for AKS

### Cost

Allowed VM SKUs

Allowed Storage SKUs

# How does it work?



User

Code

Resource Config Request

ARM – Centralized Control Plane

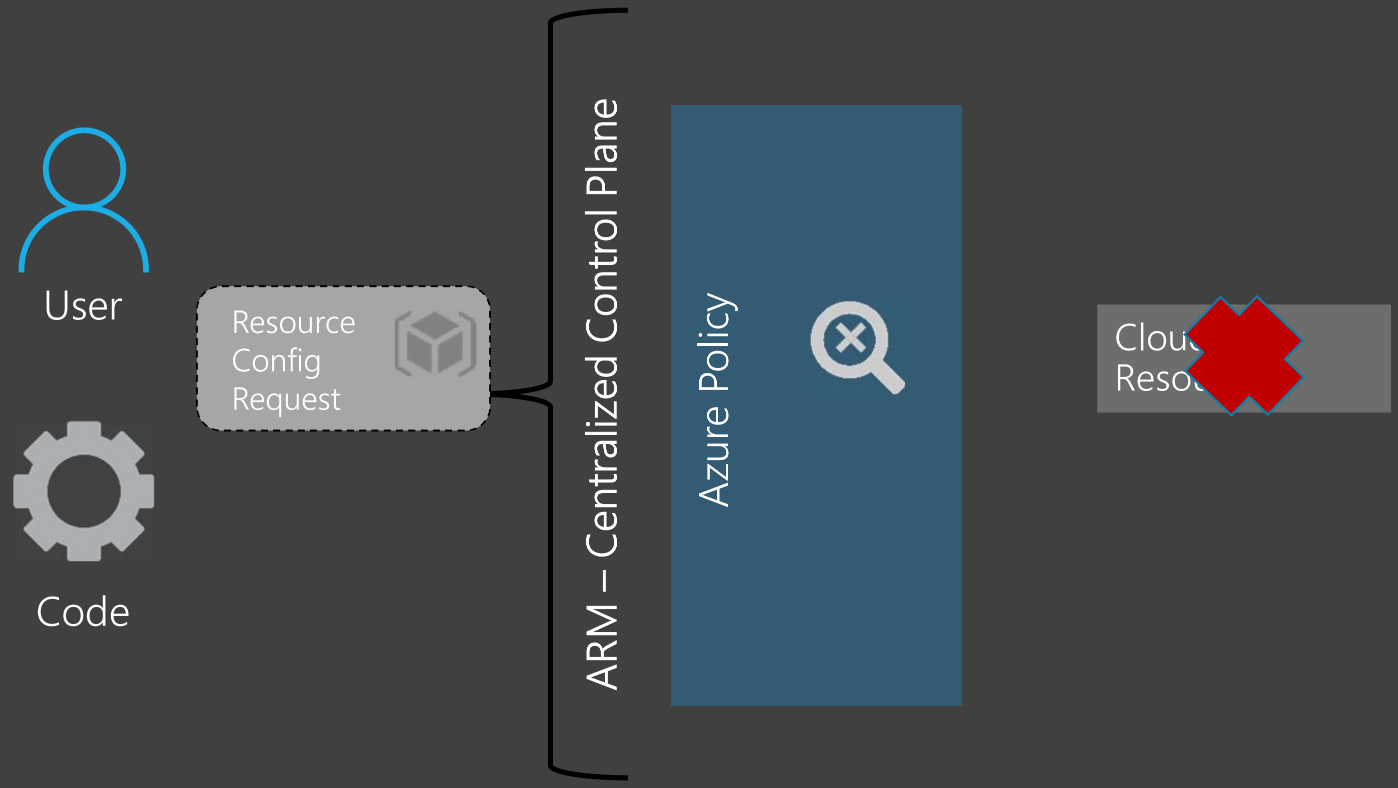
Azure Policy

Cloud Resource

## Order of evaluation

1. Append
2. Audit
3. AuditIfNotExists (on the fly)
4. Deny
5. DeployIfNotExists (check after 15 min)

# How does it work?



- AAppend
- udit
- AuditIfNotExists (on the fly)
- Deny
- DeployIfNotExists (check after 15 min)

# Azure Policy

DEMO

# Azure Security Center

# *Azure Security Center*

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

# Azure Security Center

## Strengthen security posture

**Cloud security posture management**

Secure Score

Policies and compliance

## Protect against threats

For servers

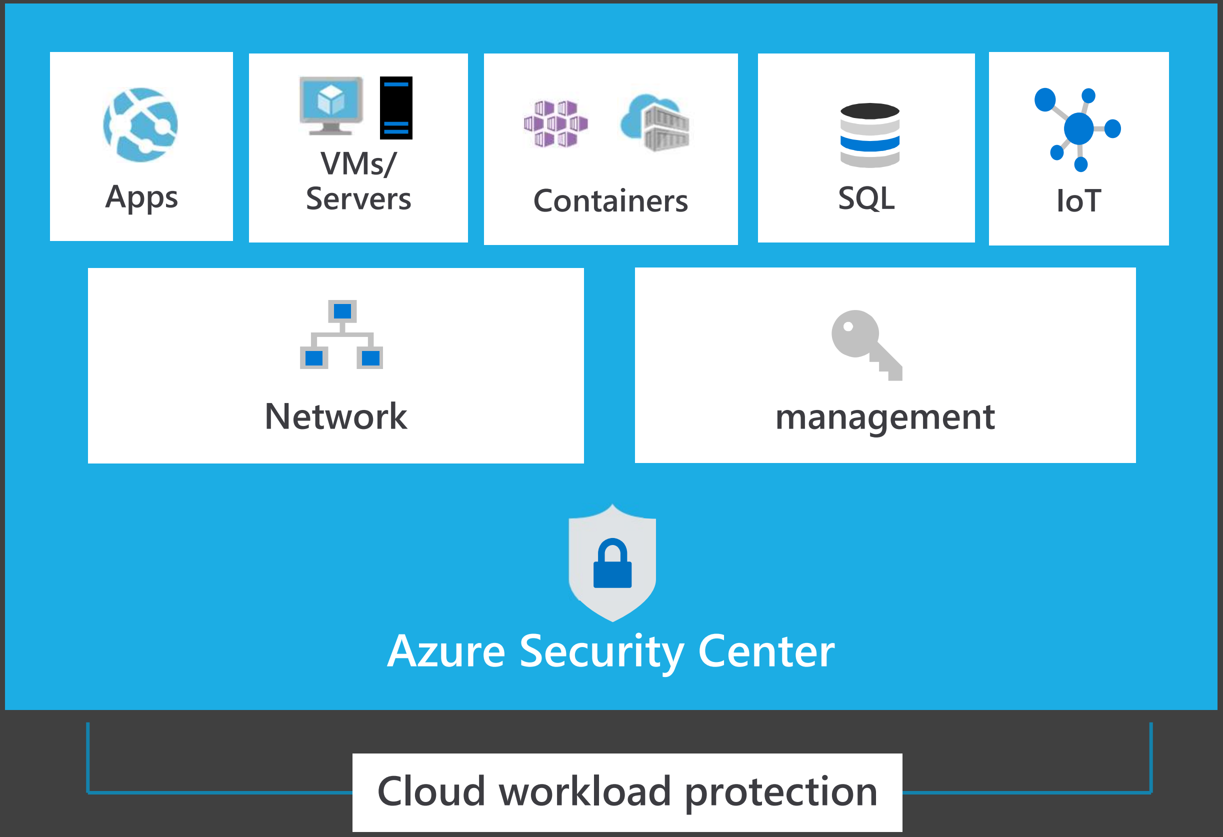
For cloud native workloads

For databases and storage

Get secure faster

# Azure Security Center

- 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

# *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
- Azure Policy settings for ASC will firstly applied when Subscription is created

# 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 RBAC, Policies and more at Higher level
- Use Deny effect for Production workloads with wisdom
- Creating initivatives even for single policy definition
- Integrate Azure Policy in your regulary Azure check

# Azure Security Center recap

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 REGULARY 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/
- https://github.com/Azure/Azure-Security-Center
- https://techcommunity.microsoft.com/t5/azure-security-center/weekly-secure-score-progress-report/ba-p/2159354
- https://github.com/Azure/Azure-Security-Center/tree/master/Secure%20Score/SecureScoreOverTimeReport
- Training: https://aka.ms/ascninja
- Videos: https://aka.ms/ascinthefiled
- ASC Lab: https://aka.ms/aslabs

#ScottishSummit2021

Questions? ->
Reach me via Twitter ☺

SCOTTISH SUMMIT

Thank You

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