Azure Governance

Eric Berg

- Lead Architect – Team Azure
- Azure, Datacenter and Modern Workplace
- Azure, System Center, Windows Server and Client
- info@ericberg.de
- @ericberg_de | @GeekZeugs
- www.ericberg.de | www.geekzeugs.de

MOUNTAIN IT
www.ericberg.de

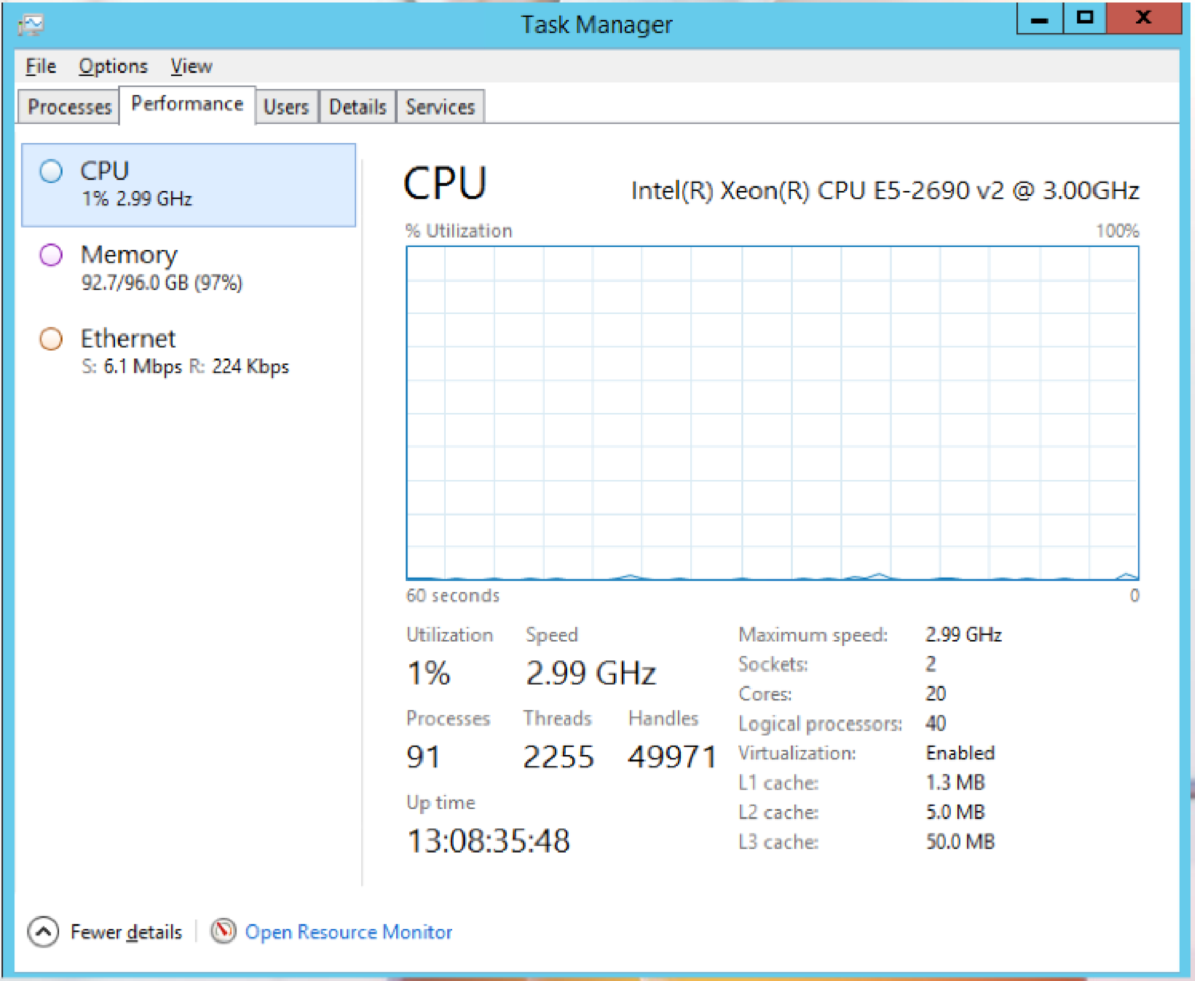
MVP Microsoft® Most Valuable Professional

GEEKZEUGS HOME OF
GEEKSPRECH Podcast
GEEKSCHAU Webcast
GEEKTREFF Community

Azure Meetup THÜRINGEN

EXAMPLES – NOTHING NEW ☺

- Never touch a running system



CPU
1% 2.99 GHz

Memory
92.7/96.0 GB (97%)

Ethernet
S: 6.1 Mbps R: 224 Kbps

CPU Intel(R) Xeon(R) CPU E5-2690 v2 @ 3.00GHz

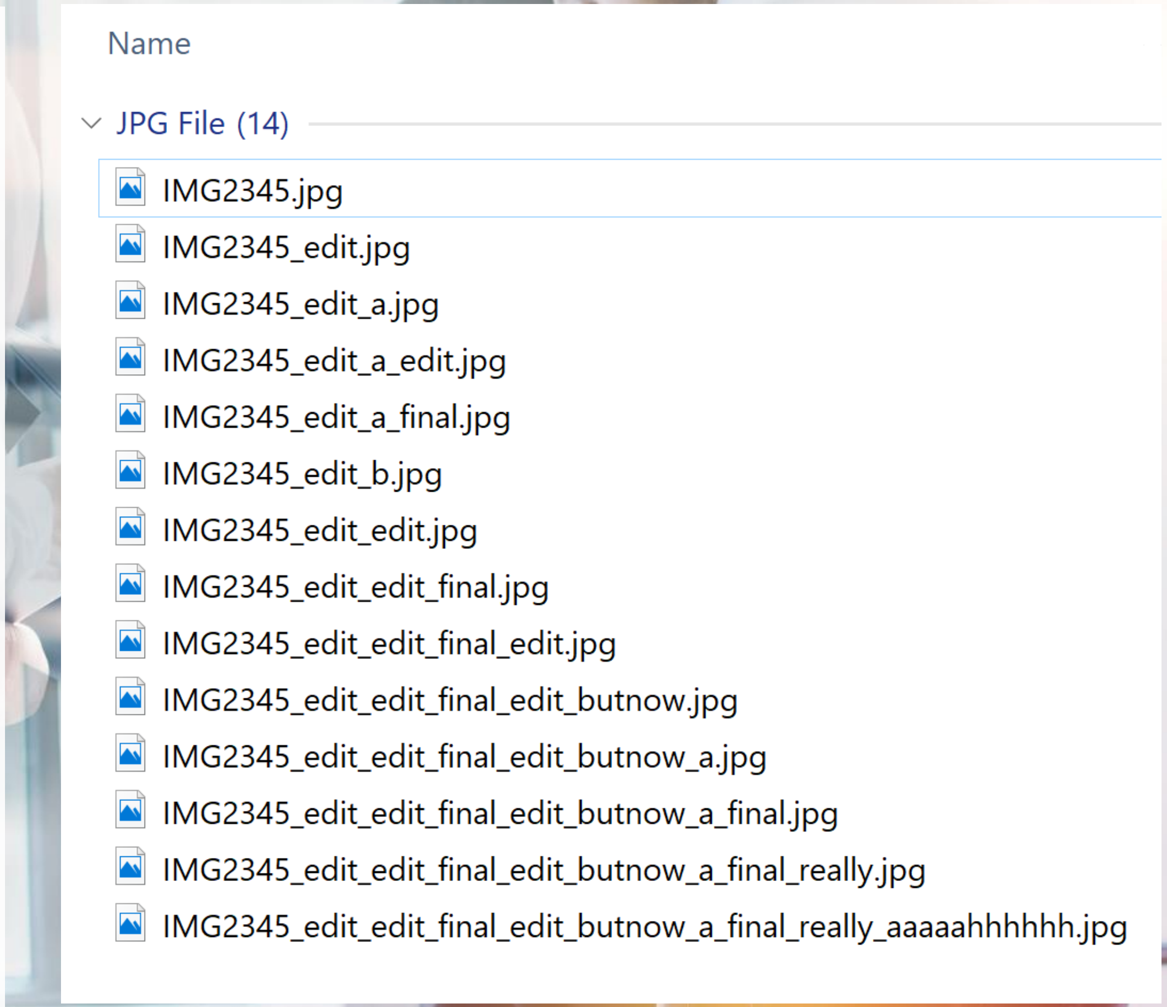
% Utilization 100%

60 seconds 0

```
Utilization   Speed                  Maximum speed:        2.99 GHz
1%            2.99 GHz               Sockets:              2
                                     Cores:                20
Processes     Threads    Handles     Logical processors:   40
91            2255       49971       Virtualization:       Enabled
                                     L1 cache:             1.3 MB
Up time                              L2 cache:             5.0 MB
13:08:35:48                          L3 cache:             50.0 MB
```

EXAMPLES – NOTHING NEW ☺

- Never touch a running system
- Never touch an old file



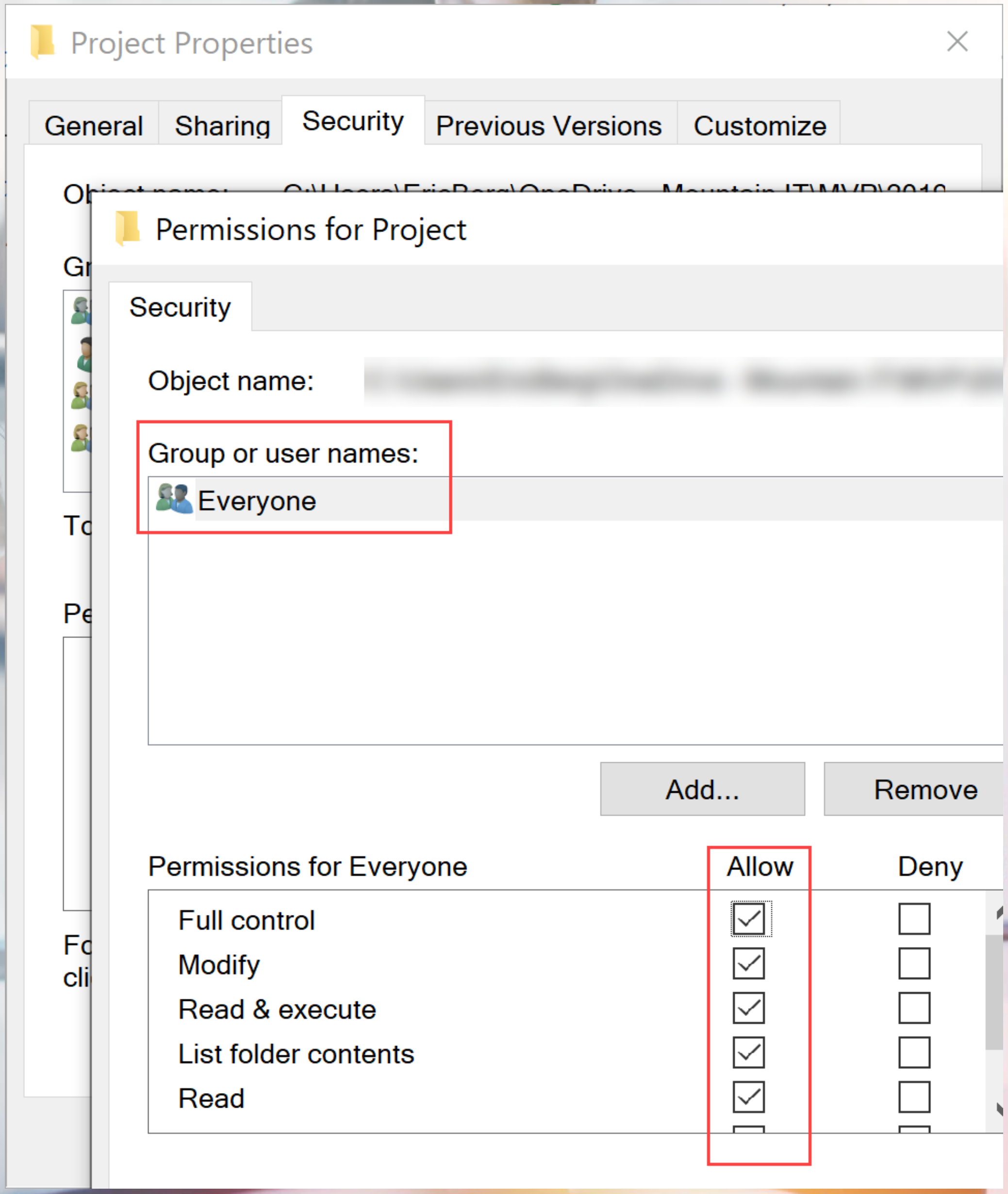
Name

JPG File (14)

IMG2345.jpg
IMG2345_edit.jpg
IMG2345_edit_a.jpg
IMG2345_edit_a_edit.jpg
IMG2345_edit_a_final.jpg
IMG2345_edit_b.jpg
IMG2345_edit_edit.jpg
IMG2345_edit_edit_final.jpg
IMG2345_edit_edit_final_edit.jpg
IMG2345_edit_edit_final_edit_butnow.jpg
IMG2345_edit_edit_final_edit_butnow_a.jpg
IMG2345_edit_edit_final_edit_butnow_a_final.jpg
IMG2345_edit_edit_final_edit_butnow_a_final_really.jpg
IMG2345_edit_edit_final_edit_butnow_a_final_really_aaaaahhhhhh.jpg

EXAMPLES – NOTHING NEW ☺

- Never touch a running system
- Never touch an old file
- There are never enough rights



Object name: C:\Users\EricBerg\OneDrive - Mountain IT\MVP\2016

Permissions for Project

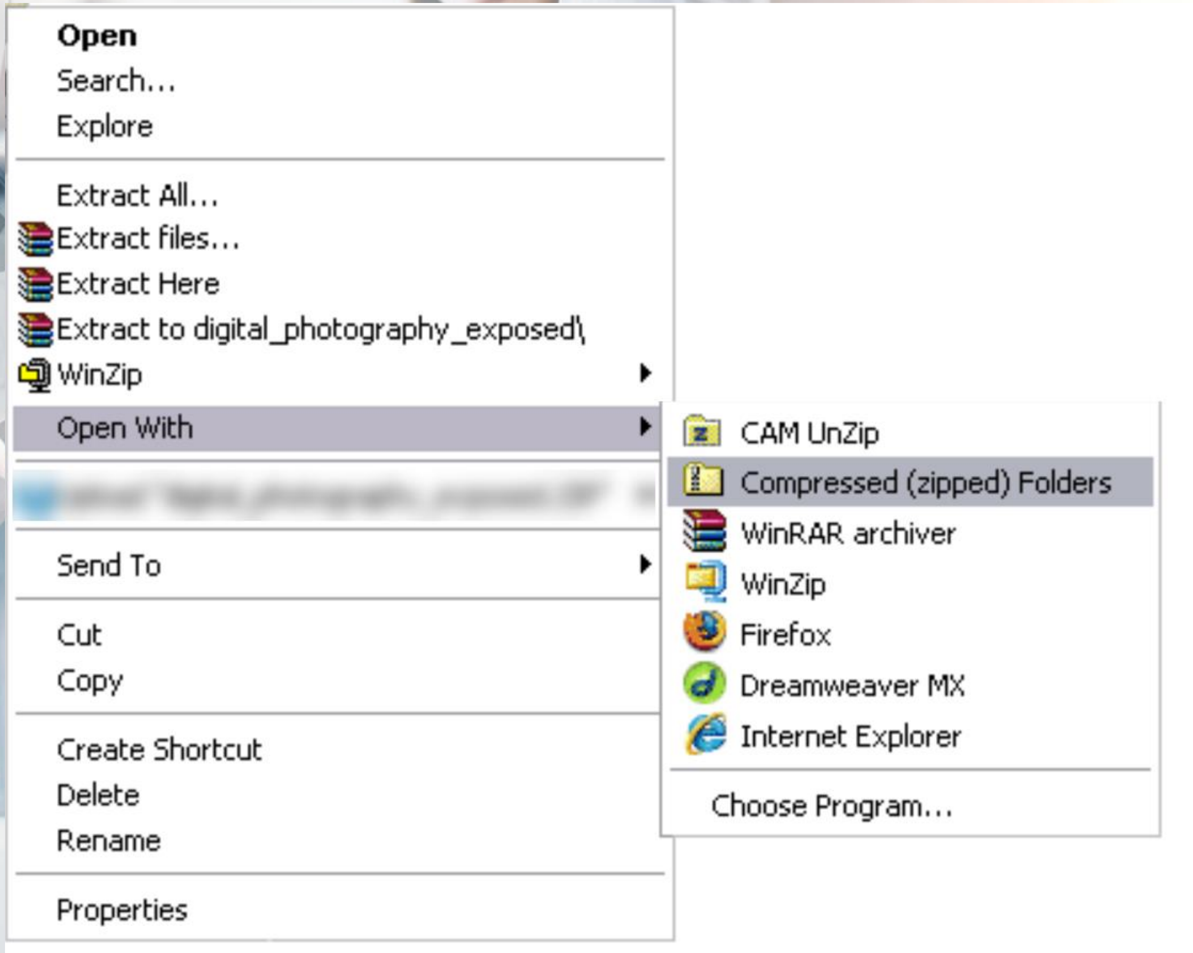
Object name: [redacted]

Group or user names:
Everyone

Permissions for Everyone	Allow	Deny
Full control	☑	□
Modify	☑	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□

EXAMPLES – NOTHING NEW ☺

- Never touch a running system
- Never touch an old file
- There are never enough rights
- Use the right tool
- …



Cloud Governance

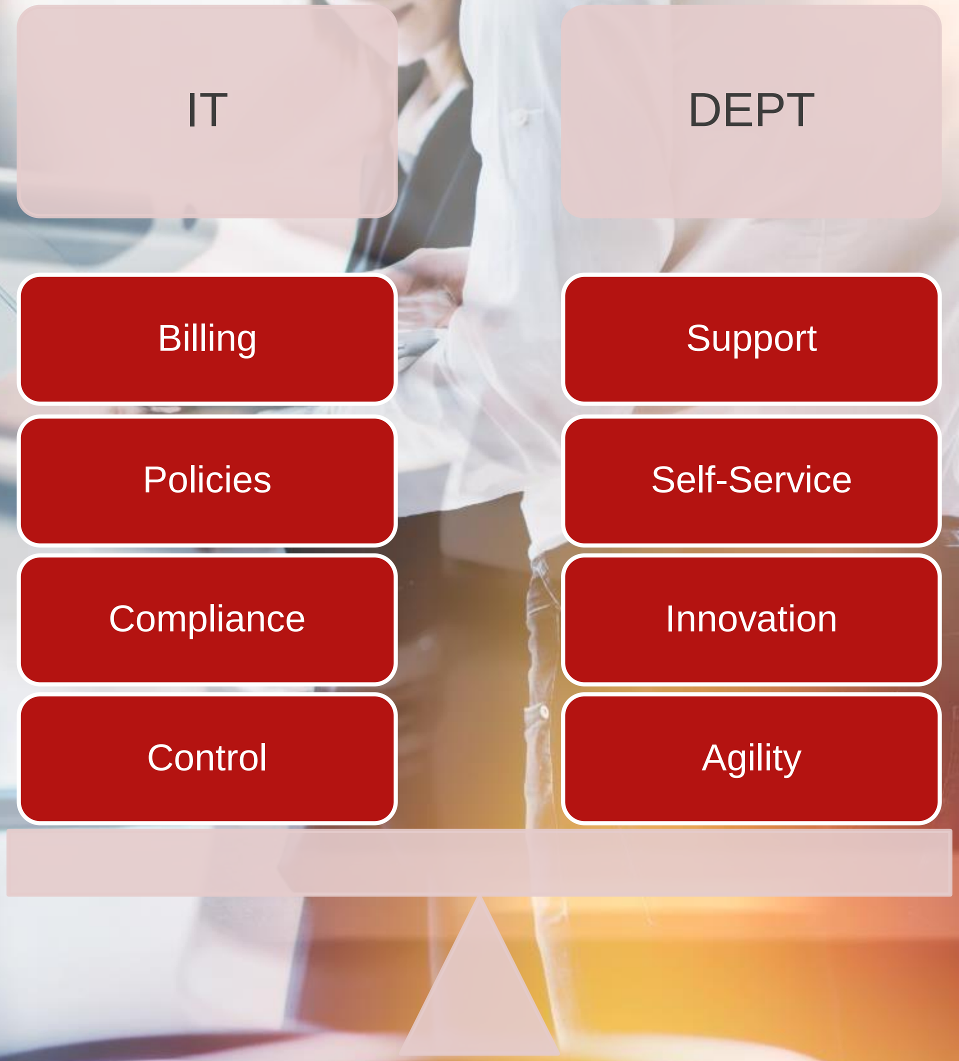
ESTABLISHMENT of **POLICIES** and continuous **MONITORING** of their proper **IMPLEMENTATION**, by the members of the governing body of an organization

[...]

Source: www.businessdictionary.com

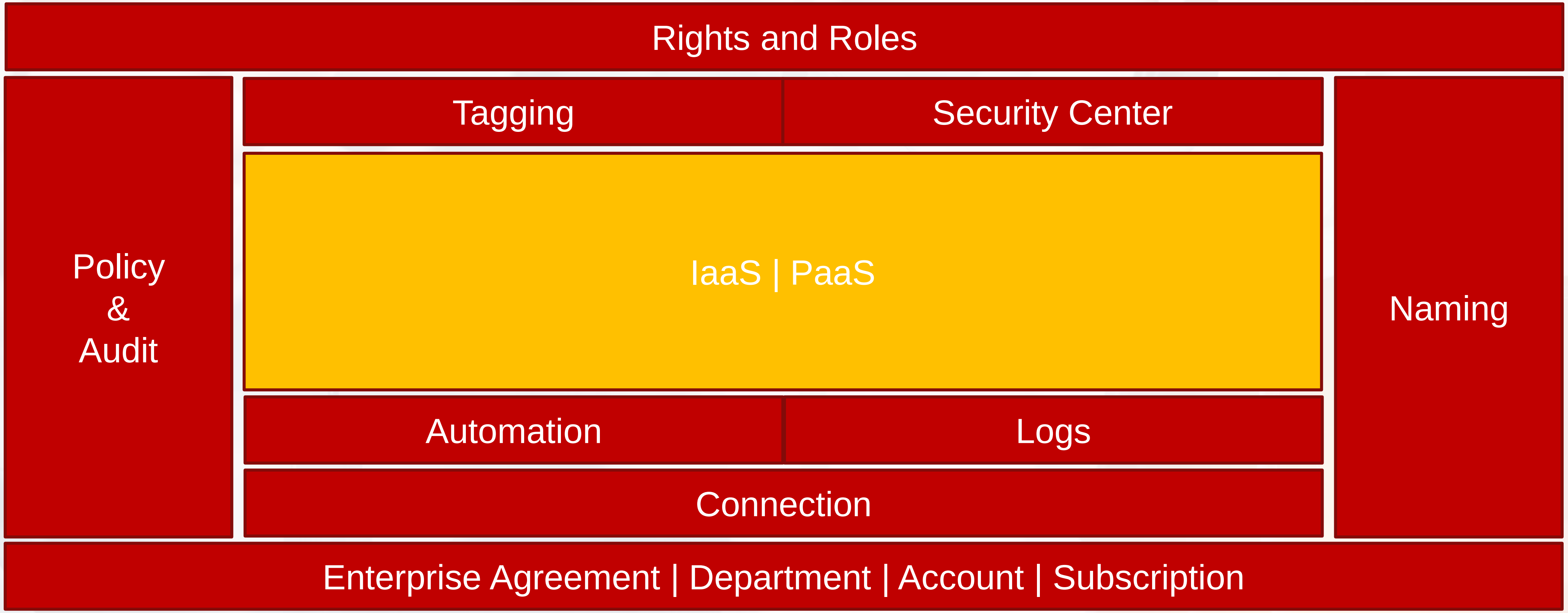
Requirements

- Cloud is (not) an IT topic
- Cloud usage is already there
- IT as trusted advisor in business
- Avoid shadow cloud
- Achieve more with business



IT	DEPT
Billing	Support
Policies	Self-Service
Compliance	Innovation
Control	Agility

Azure Governance



Rights and Roles

Policy & Audit

Tagging

Security Center

IaaS | PaaS

Automation

Logs

Connection

Naming

Enterprise Agreement | Department | Account | Subscription

Azure Security & Management

Governance

NEW

Proactively apply policies and optimize cloud spend

Security

Industry leading Security with Advanced Threat Protection

Resiliency

High availability and protection for VMs, apps and data

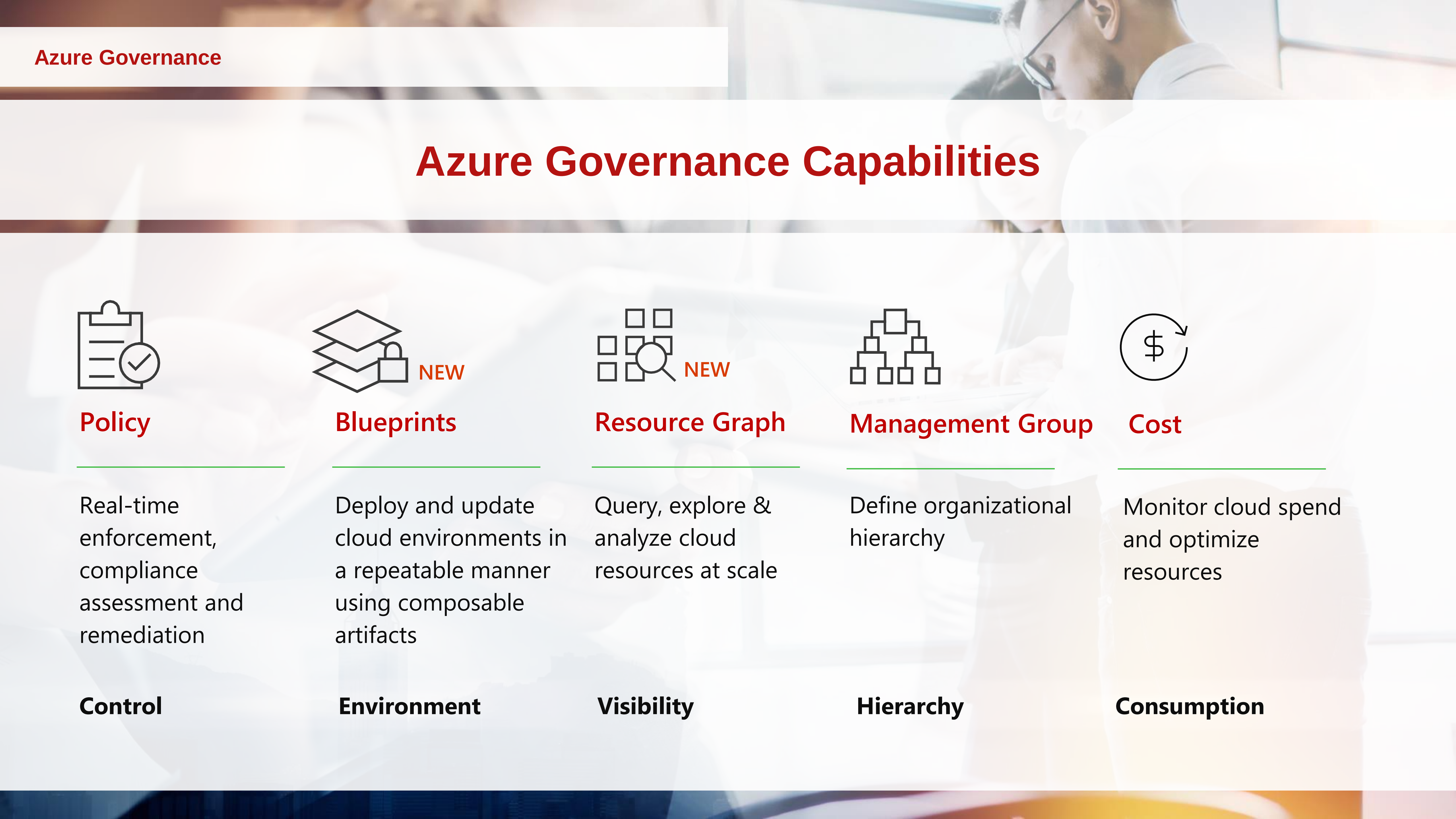
Monitoring

Deep operational insights with rich intelligence

Automate

Powerful scripting, configuration and update management

Built-in Azure services options to keep your Azure and hybrid resources secure and well-managed



Azure Governance Capabilities

Policy

Real-time enforcement, compliance assessment and remediation

Control

Blueprints

NEW

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

Environment

Resource Graph

NEW

Query, explore & analyze cloud resources at scale

Visibility

Management Group

Define organizational hierarchy

Hierarchy

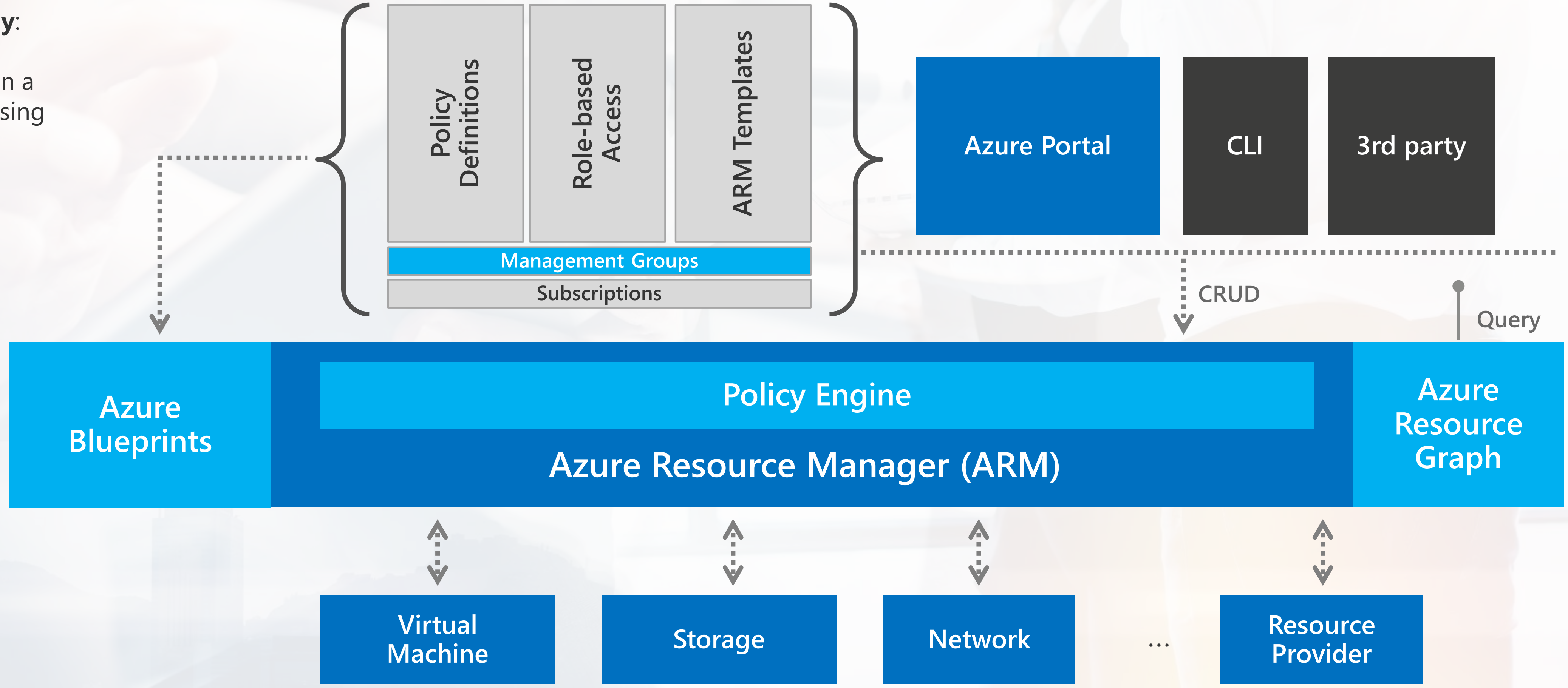
Cost

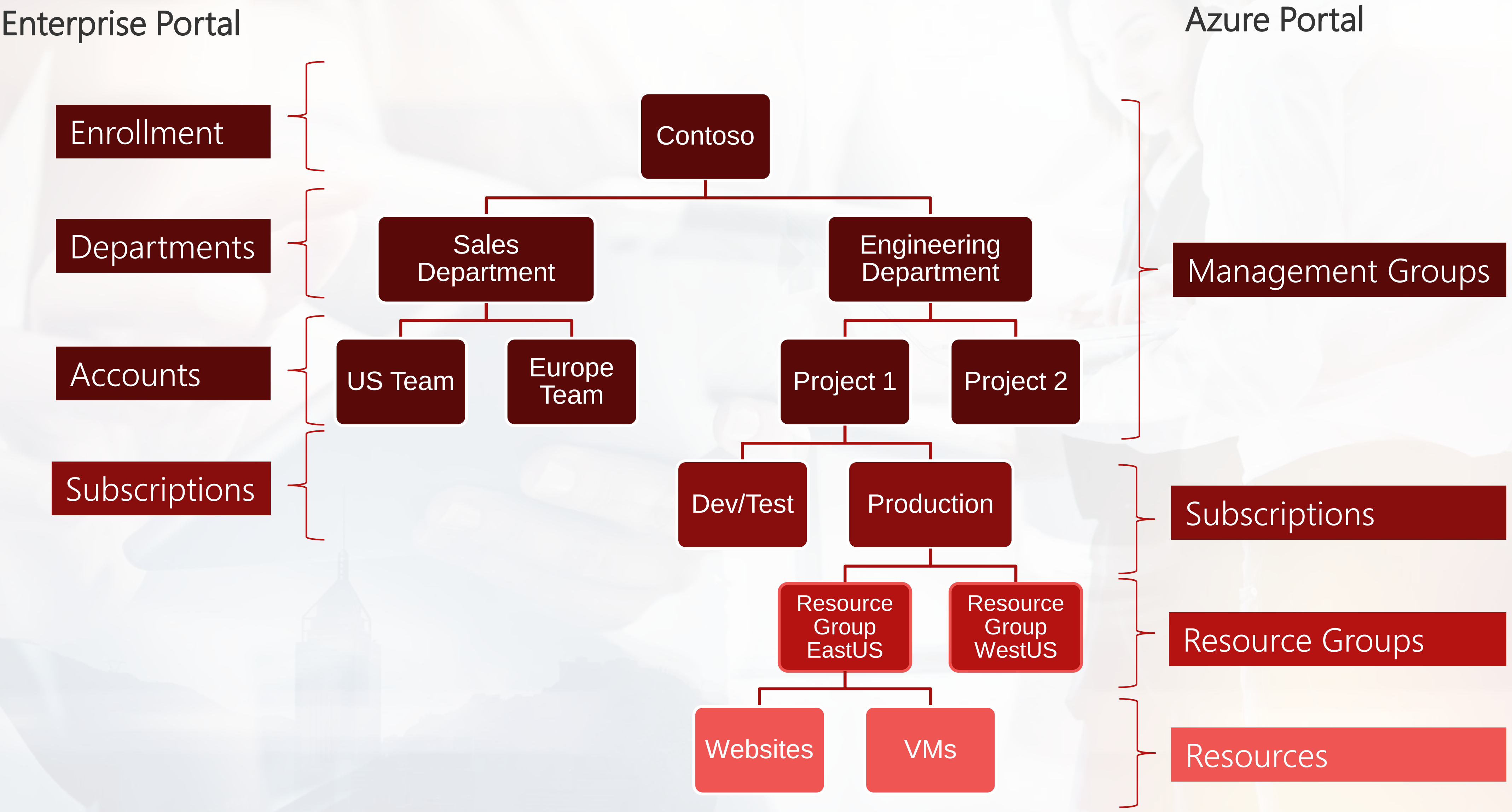
Monitor cloud spend and optimize resources

Consumption

Azure Governance Architecture

1. **Environment Factory**: Deploy and update cloud environments in a repeatable manner using composable artifacts



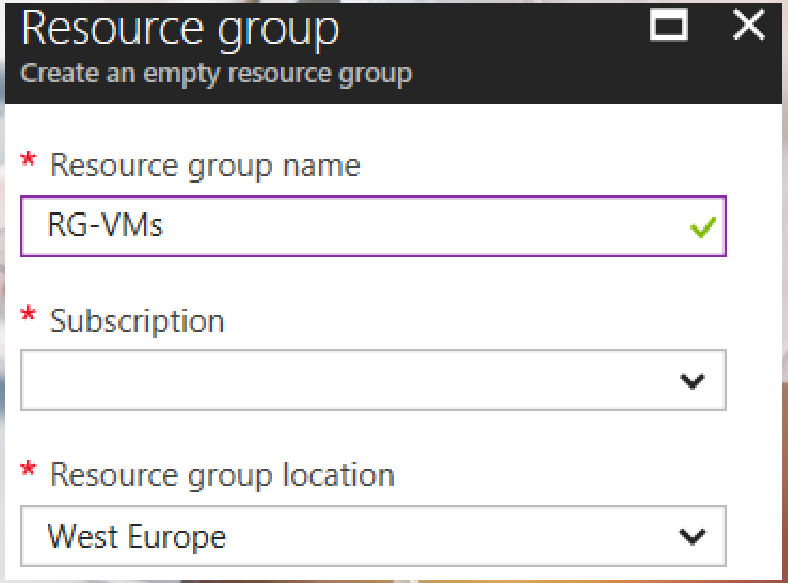

Enterprise Portal
Azure Portal
Enrollment
Departments
Accounts
Subscriptions
Contoso
Sales Department
Engineering Department
US Team
Europe Team
Project 1
Project 2
Dev/Test
Production
Resource Group EastUS
Resource Group WestUS
Websites
VMs
Management Groups
Subscriptions
Resource Groups
Resources

Resource Groups

> *“It is good to collect things, but it is better to go on walks.”*
>
> *- Anatole France*

Resource Group

- RGs = container for resources
- Every resource is member of a RG
- Every resource has only one RG
- RGs cannot be encapsulated
- RGs stick to a region



Resource group

Create an empty resource group

* Resource group name

RG-VMs ✓

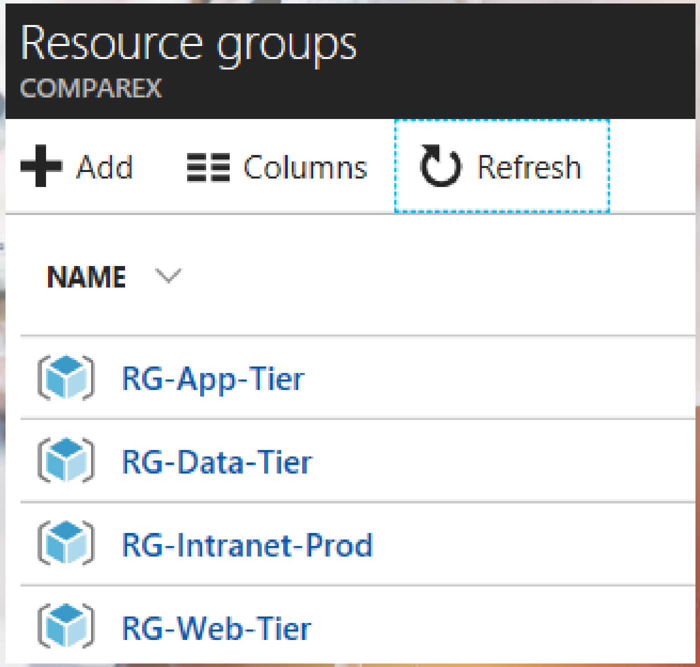
* Subscription

* Resource group location

West Europe

Resource Group

- Decide when to create a RG
- Traditional
  - Same lifecycle
  - APP-Management
- Agile
  - Deployment-Layer
  - Web, App, DB
- Decide and stick through



Resource groups

COMPAREX

NAME

RG-App-Tier

RG-Data-Tier

RG-Intranet-Prod

RG-Web-Tier

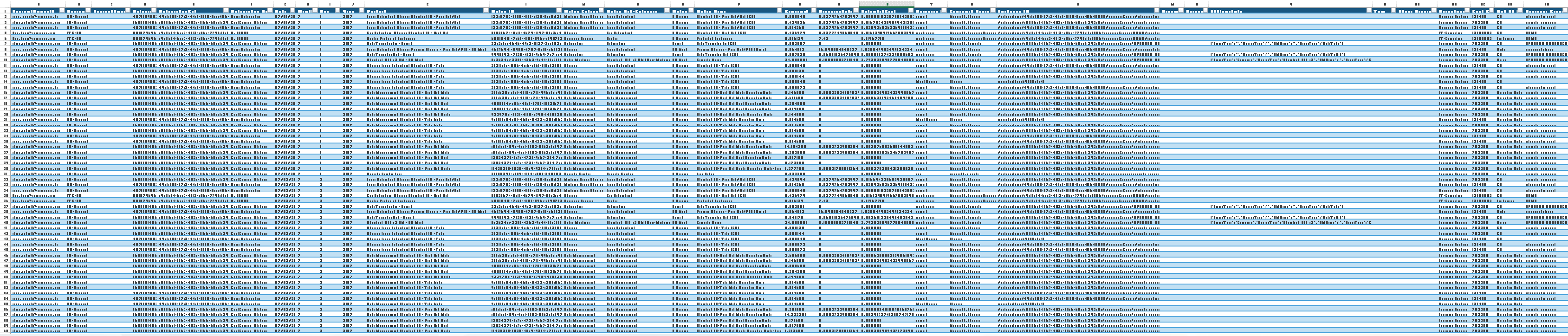
Resource Tags

“Decide that you want it more than you are afraid of it.”

- Unknown

Resource Tags

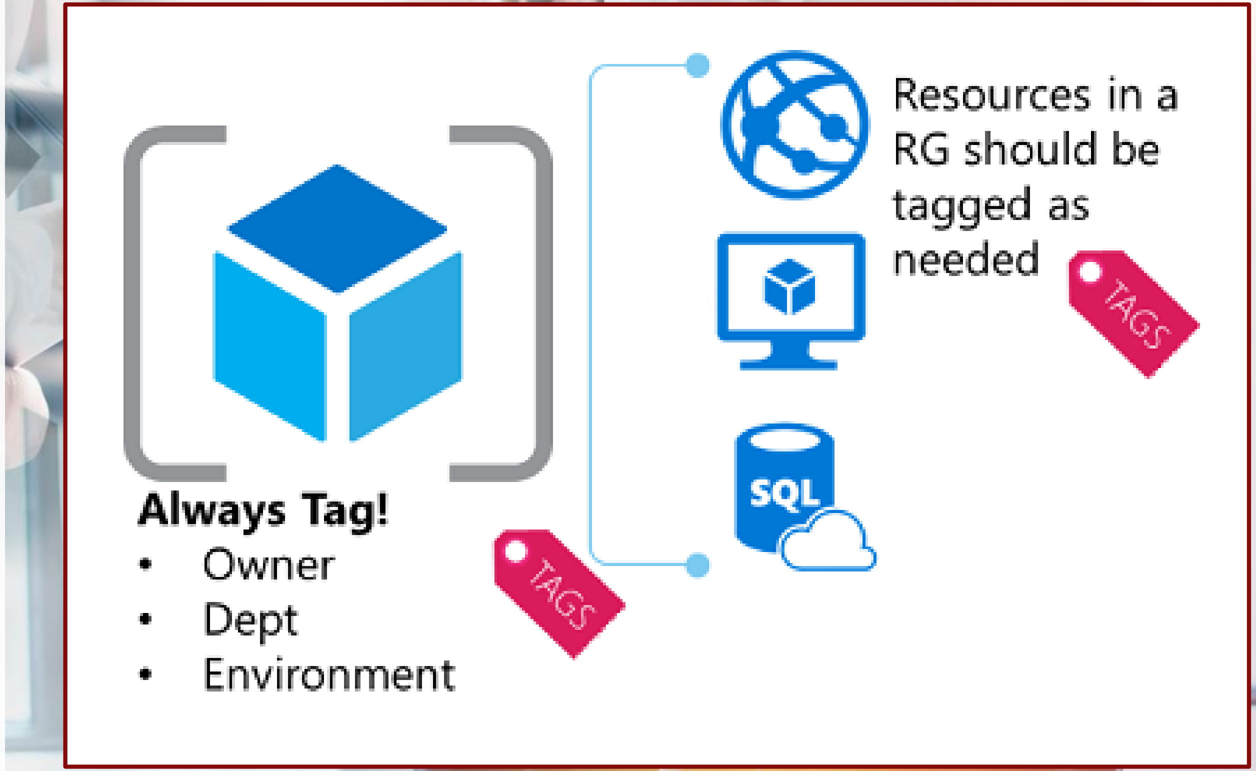
- Billing in Azure difficult
- List of resource cost



Resource Tags

- Property : Value
- Tags help to assign cost / responsibility
- Always tag RGs
  - Owner
  - Department
  - Environment
- Other ressources as required

- Tags are your friends!
- Define tags in advance!
- Tag in Template!



Always Tag!

- Owner
- Dept
- Environment

Resources in a RG should be tagged as needed

Resource Policies

“You are remembered for the rules you break.”

- Douglas MacArthur

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

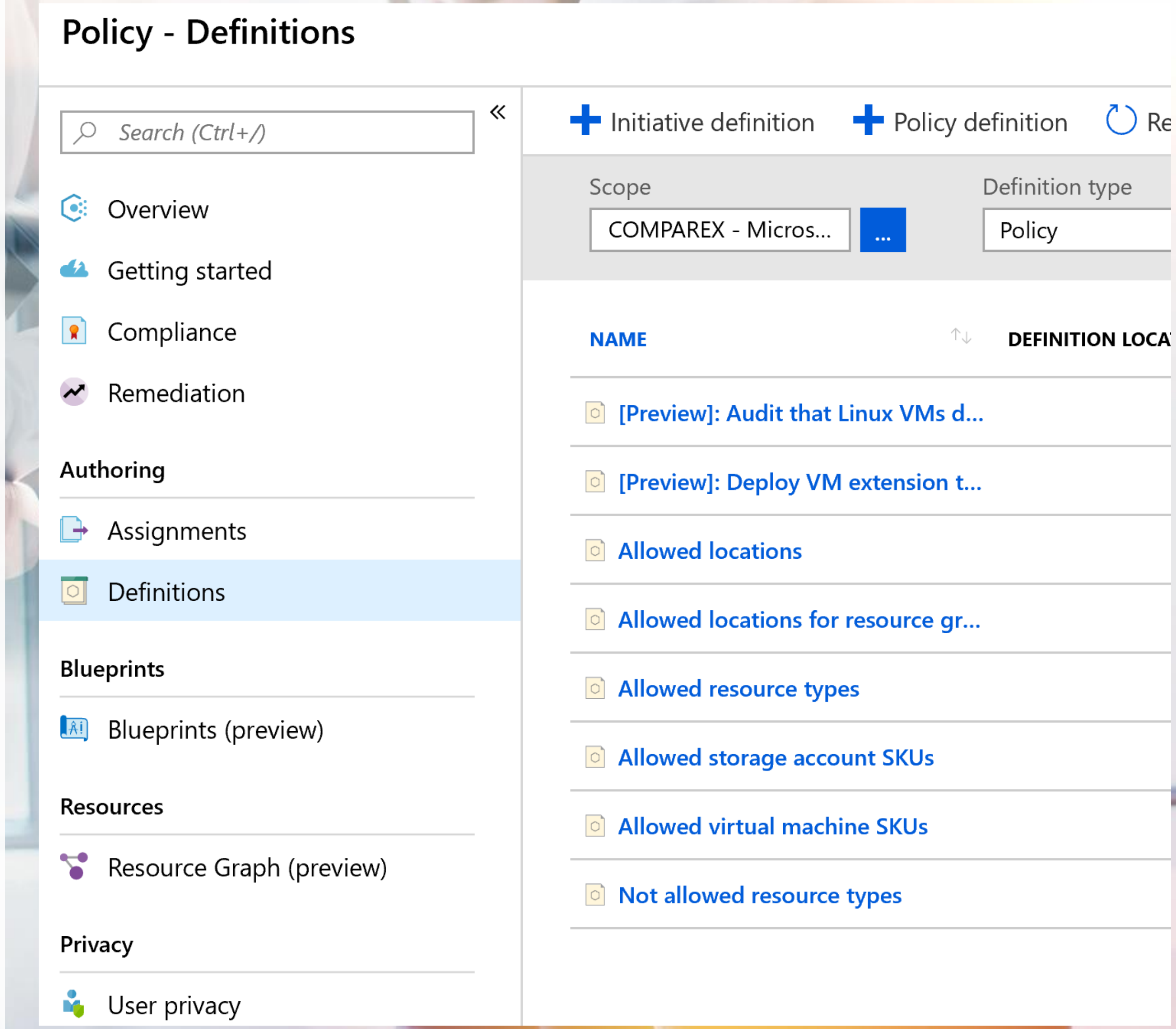
Apply policies at scale

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

Remediation

Resource Policies

- Set of rules for Subscriptions or RGs
- Policy is the Allow System
- If-then conditions
- Created via JSON
- Actions:
  - Deny
  - Audit
  - Append



Policy - Definitions

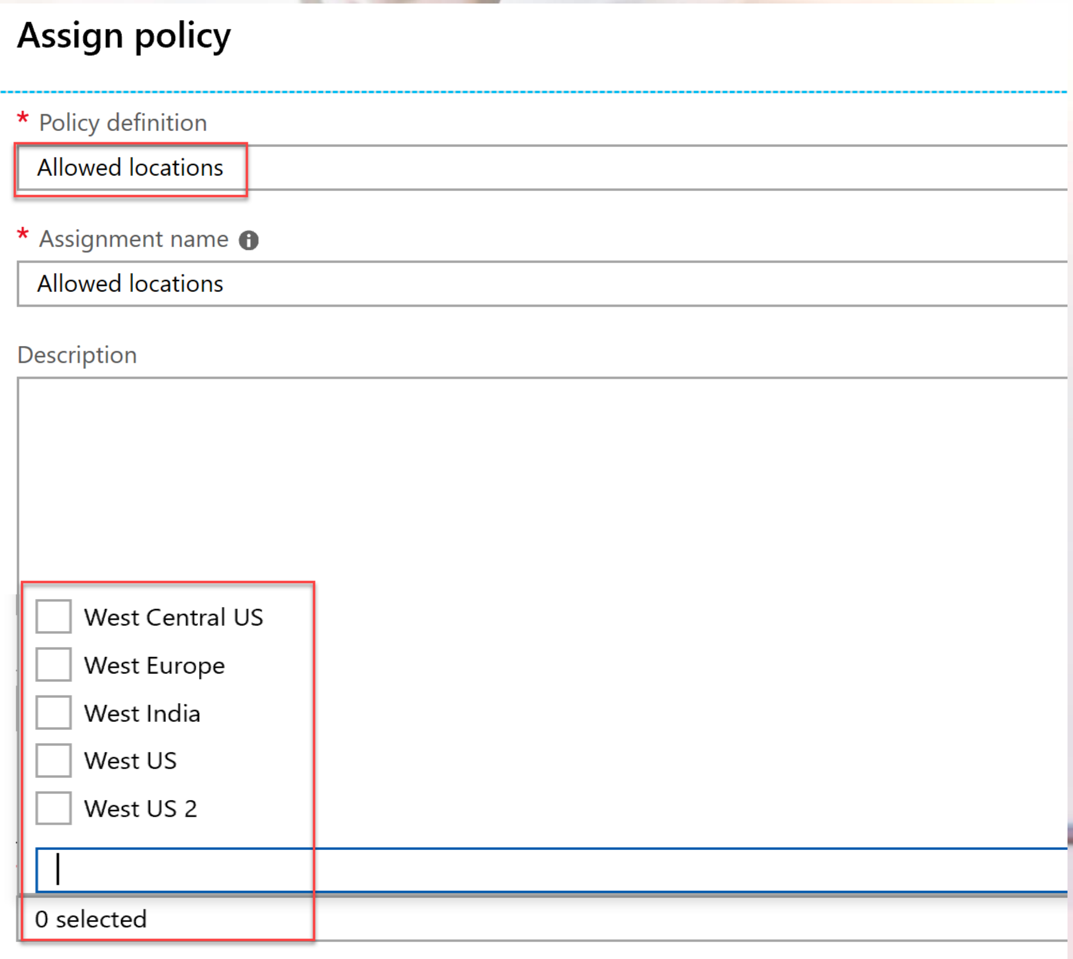
Scope: COMPAREX - Micros...

Definition type: Policy

NAME	DEFINITION LOCA
[Preview]: Audit that Linux VMs d...	
[Preview]: Deploy VM extension t...	
Allowed locations	
Allowed locations for resource gr...	
Allowed resource types	
Allowed storage account SKUs	
Allowed virtual machine SKUs	
Not allowed resource types	

Resource Policies

- Define Subscription Policies for:
  - Geo-compliance/data sovereignty
  - Cost management
  - Required tags
- Audit Activities and Log them
- Use Log Analytics



Assign policy

* Policy definition

Allowed locations

* Assignment name

Allowed locations

Description

□ West Central US

□ West Europe

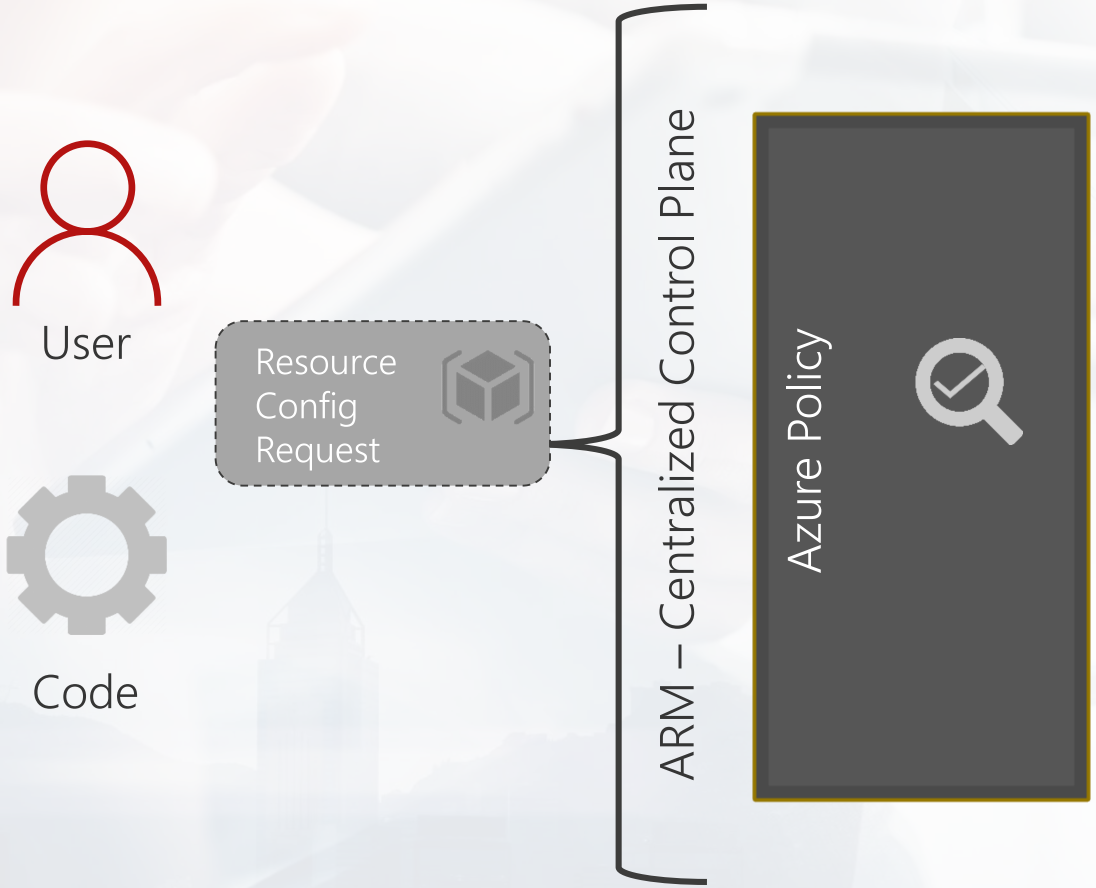
□ West India

□ West US

□ West US 2

0 selected

How does the processing work?

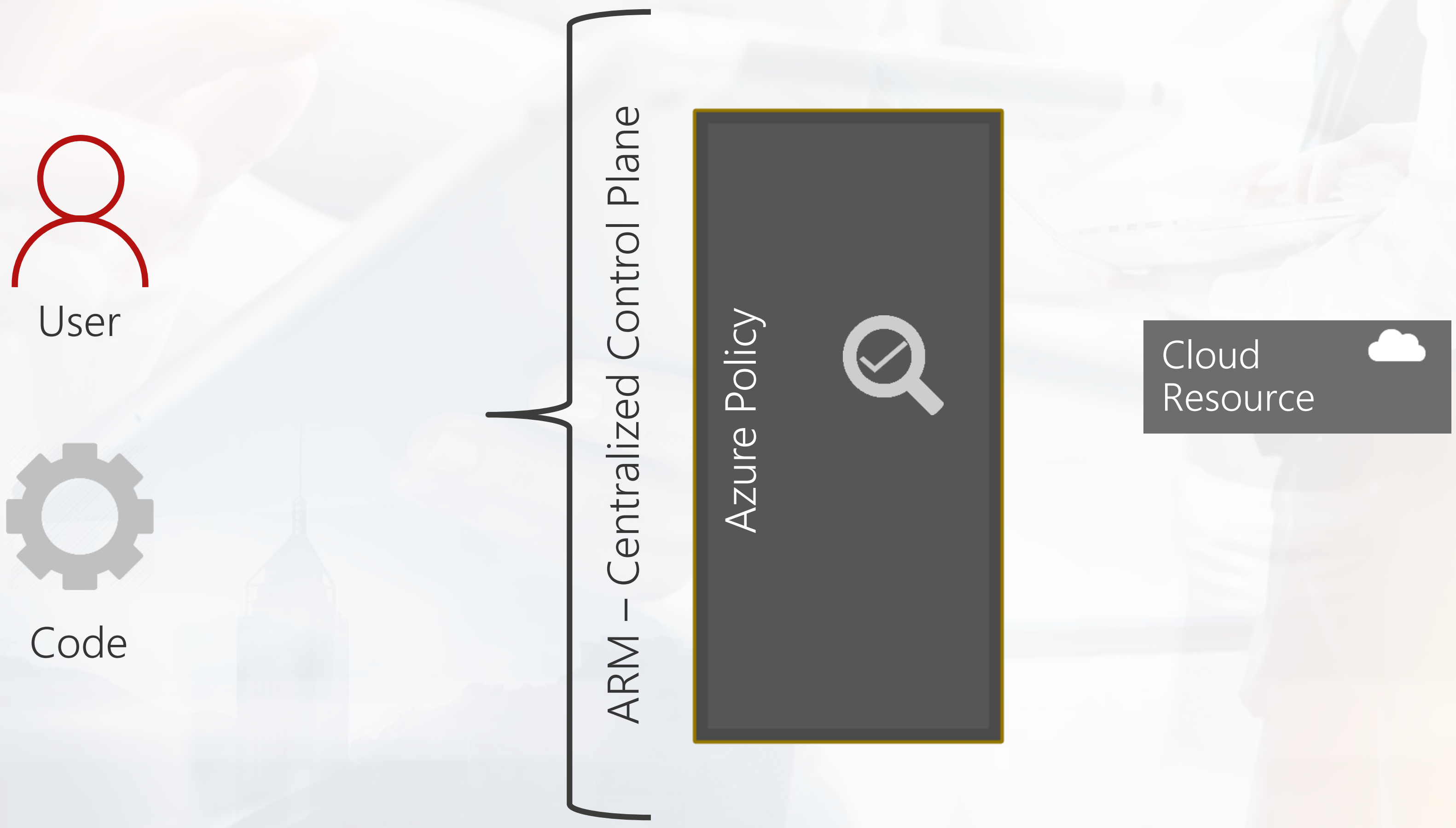


Cloud Resource

Order of evaluation

1. Append
2. Deny
3. Audit

How does the processing work?



User

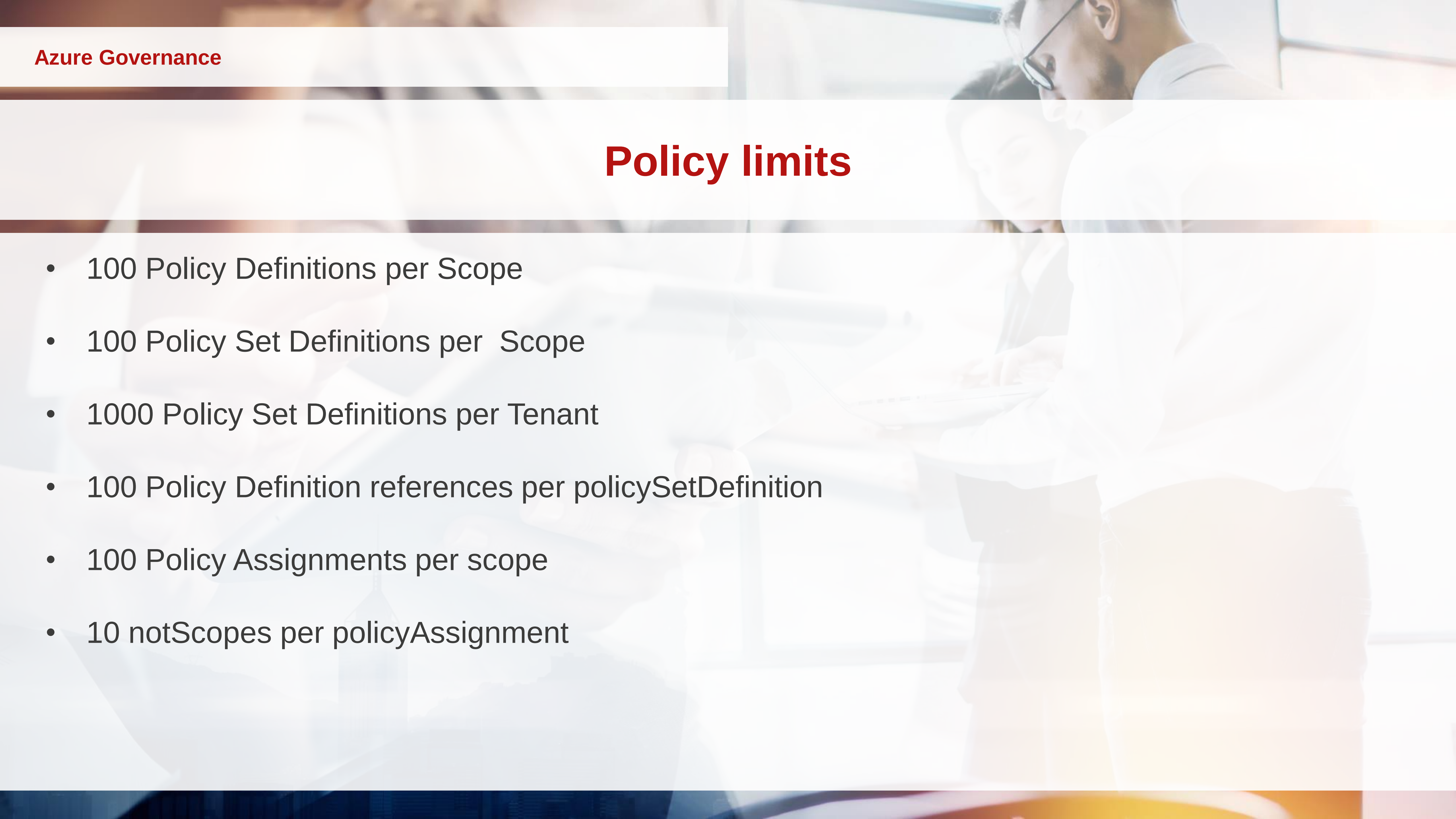
Code

ARM – Centralized Control Plane

Azure Policy

Cloud Resource

4. DeployIfNotExists
5. AuditIfNotExists

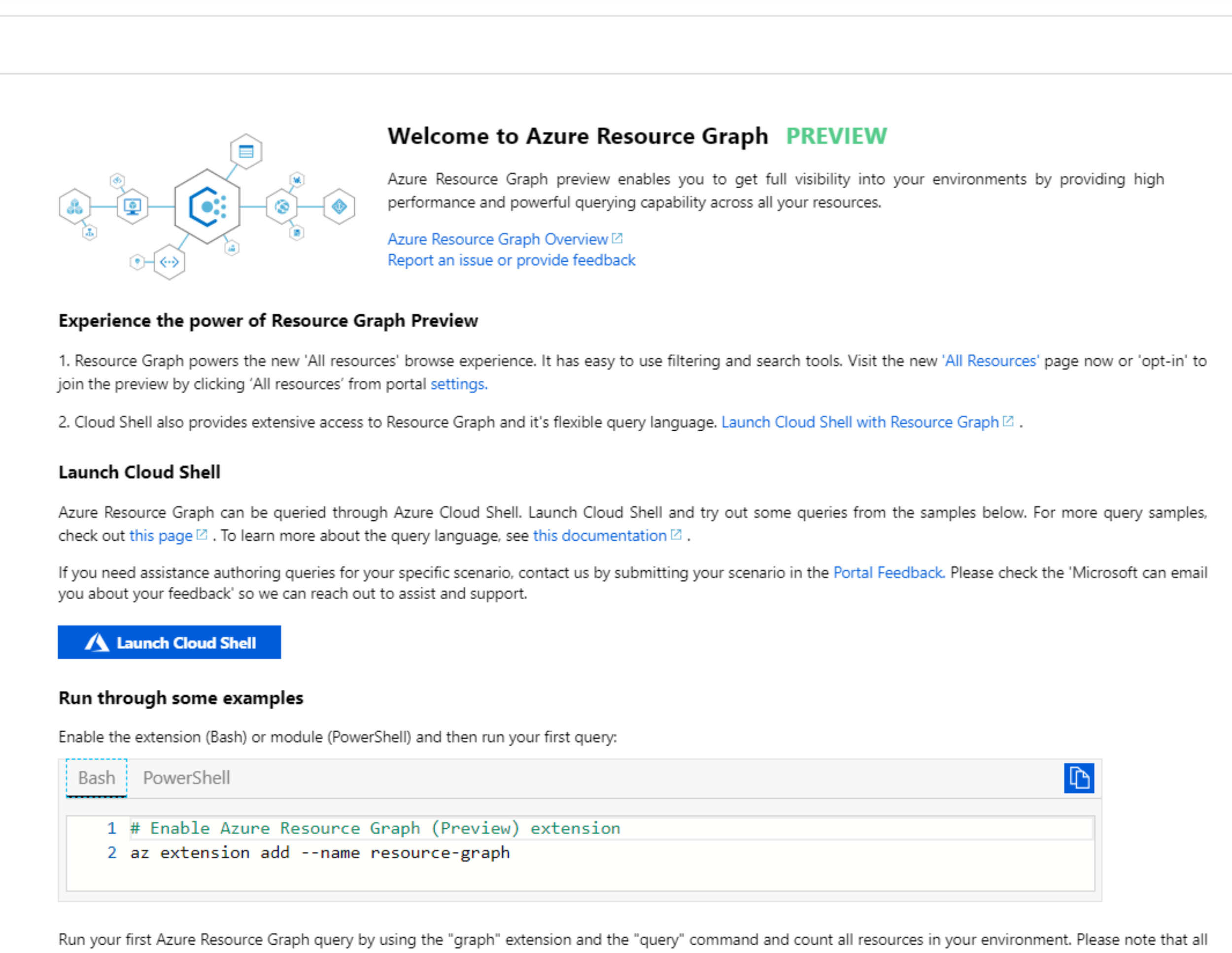


Policy limits

- 100 Policy Definitions per Scope
- 100 Policy Set Definitions per Scope
- 1000 Policy Set Definitions per Tenant
- 100 Policy Definition references per policySetDefinition
- 100 Policy Assignments per scope
- 10 notScopes per policyAssignment

Resource Graph (Preview)

- Query opportunity for resources based on a Query language
- Evaluation of the scope of the use of a policy
- Examples of queries would be:
  - Counting Azure Resources
  - Listing all resources sorted by name
  - List the resources that consume storage
  - Listing resources with a specific day
  - List of all public IP addresses
  - List of all tags



Welcome to Azure Resource Graph PREVIEW

Azure Resource Graph preview enables you to get full visibility into your environments by providing high performance and powerful querying capability across all your resources.

Azure Resource Graph Overview

Report an issue or provide feedback

Experience the power of Resource Graph Preview

1. Resource Graph powers the new 'All resources' browse experience. It has easy to use filtering and search tools. Visit the new 'All Resources' page now or 'opt-in' to join the preview by clicking 'All resources' from portal settings.

2. Cloud Shell also provides extensive access to Resource Graph and it's flexible query language. Launch Cloud Shell with Resource Graph .

Launch Cloud Shell

Azure Resource Graph can be queried through Azure Cloud Shell. Launch Cloud Shell and try out some queries from the samples below. For more query samples, check out this page . To learn more about the query language, see this documentation .

If you need assistance authoring queries for your specific scenario, contact us by submitting your scenario in the Portal Feedback. Please check the 'Microsoft can email you about your feedback' so we can reach out to assist and support.

Run through some examples

Enable the extension (Bash) or module (PowerShell) and then run your first query:

```
# Enable Azure Resource Graph (Preview) extension
az extension add --name resource-graph
```

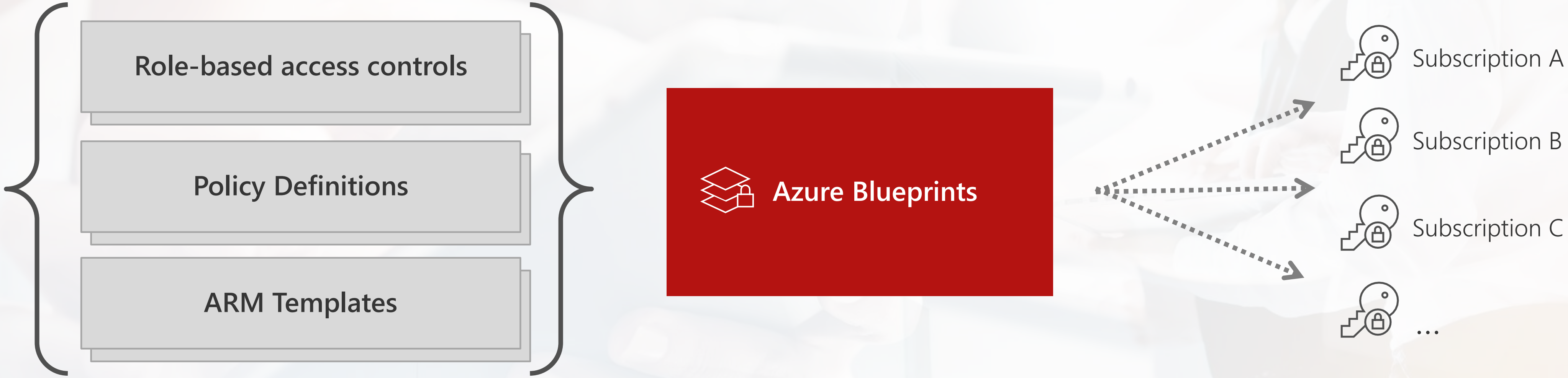
Run your first Azure Resource Graph query by using the "graph" extension and the "query" command and count all resources in your environment. Please note that all

Blueprints

“The prepared man has already won the half battle”

- Spanish statement

Azure Blueprints



Role-based access controls

Policy Definitions

ARM Templates

Azure Blueprints

Subscription A

Subscription B

Subscription C

...

Compose | Manage | Reproduce

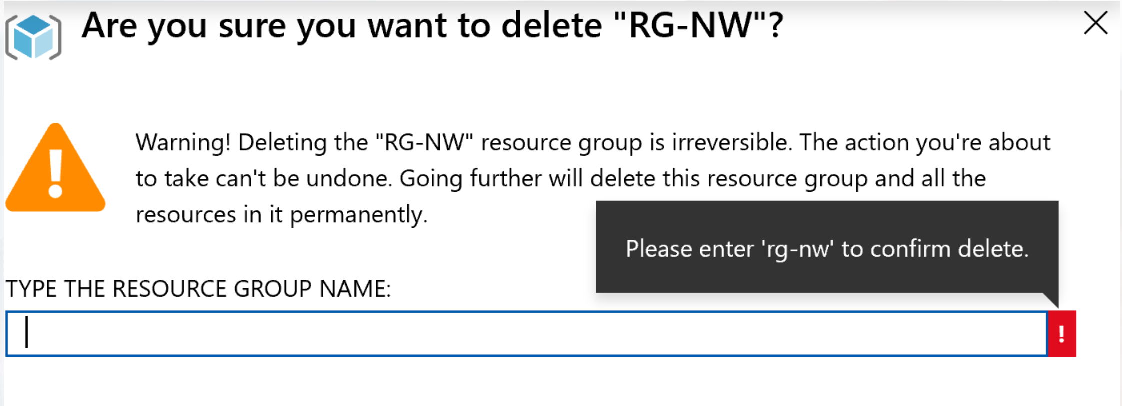
Resource Locks

“I guess what scares me the most now is the thought that I won't be able to protect you”

- Julia Hoban

Resource Locks

- Resources in Azure can be deleted easy
- Protection from Accidental Deletion
- Known from Active Directory



Are you sure you want to delete "RG-NW"?

Warning! Deleting the "RG-NW" resource group is irreversible. The action you're about to take can't be undone. Going further will delete this resource group and all the resources in it permanently.

Please enter 'rg-nw' to confirm delete.

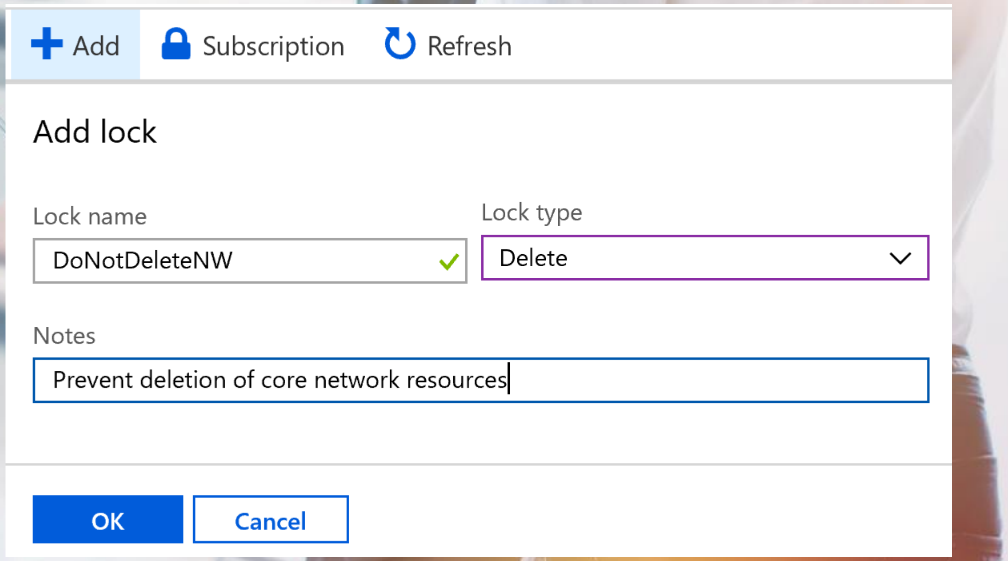
TYPE THE RESOURCE GROUP NAME:

Resource Locks

- Restrict resource access:
  - CanNotDelete
  - ReadOnly (ATTENTION)
- Set by Owner and User Access Admin

- JSON: { "properties": { "level": "CanNotDelete", "notes": "Optional text notes." } }
- PowerShell: **Set-AzureRmResourceLock**

- Locks protect!
- Define locks in advance!
- Locks in Template!



Add lock

Lock name: DoNotDeleteNW

Lock type: Delete

Notes: Prevent deletion of core network resources

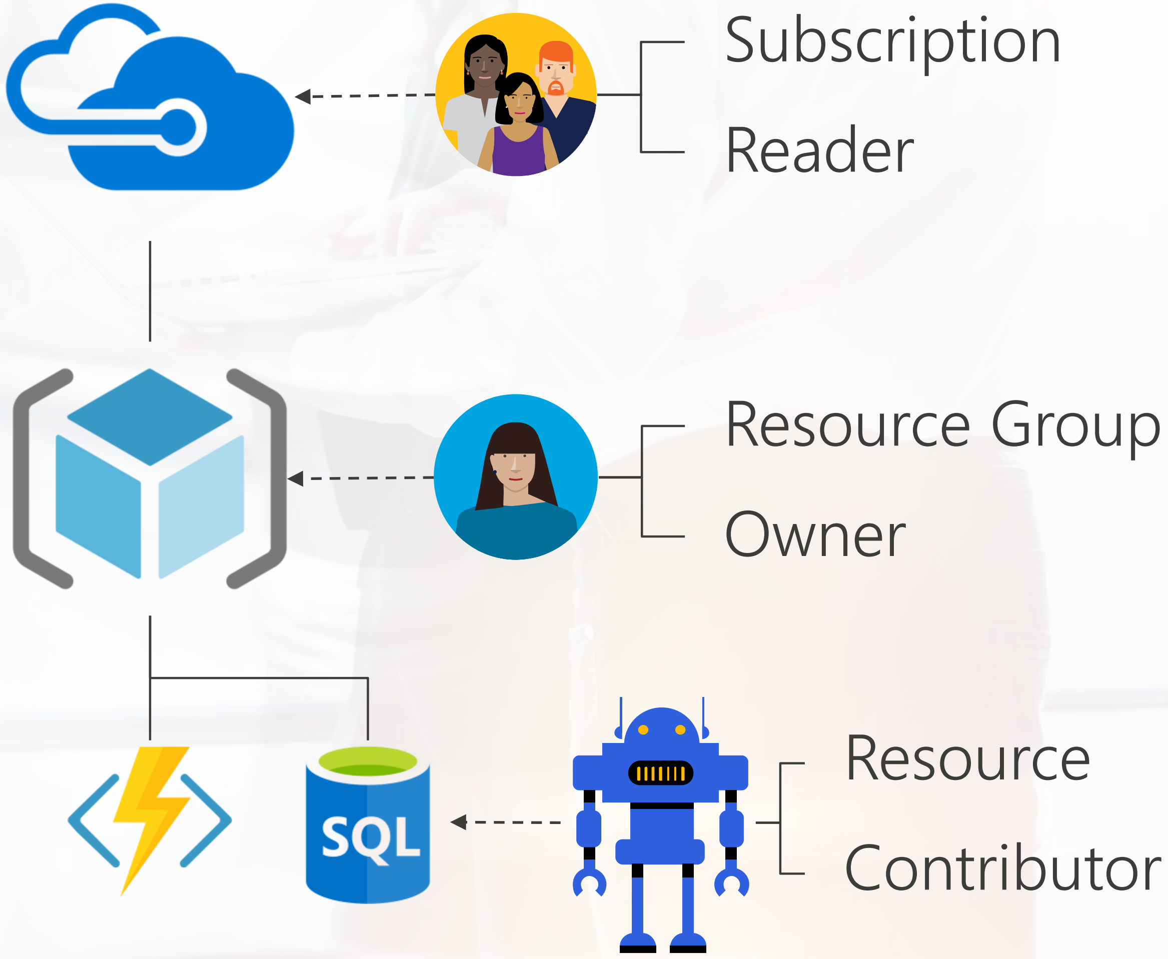
Role-Based Access Control

“Anything out there is vulnerable to attack given enough time and resources.”

- Kevin Mitnick

Role Based Access Control

- Connection between Azure AD and Subscription
- Default roles depend on
  - Owner
  - Contributor
  - Reader
- Advanced Roles
  - Automation Operator
  - DevTest Labs User
  - …
- Own roles



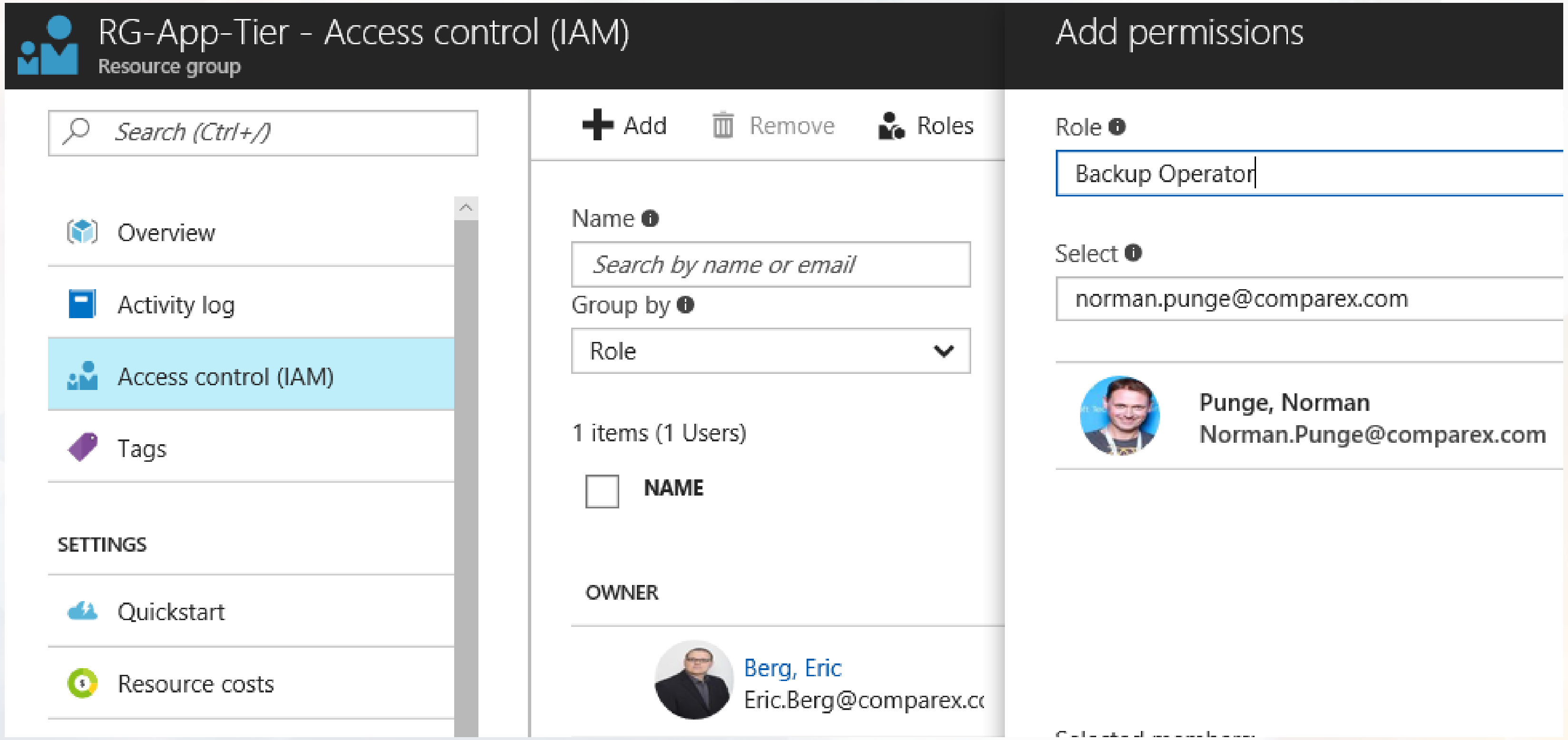
Subscription
Reader

Resource Group
Owner

Resource
Contributor

RBAC

- IAM can be set at all levels



Name: Search by name or email

Group by: Role

1 items (1 Users)

□ NAME

OWNER

Berg, Eric
Eric.Berg@comparex.cc

Role: Backup Operator

Select: norman.punge@comparex.com

Punge, Norman
Norman.Punge@comparex.com

Selected members:

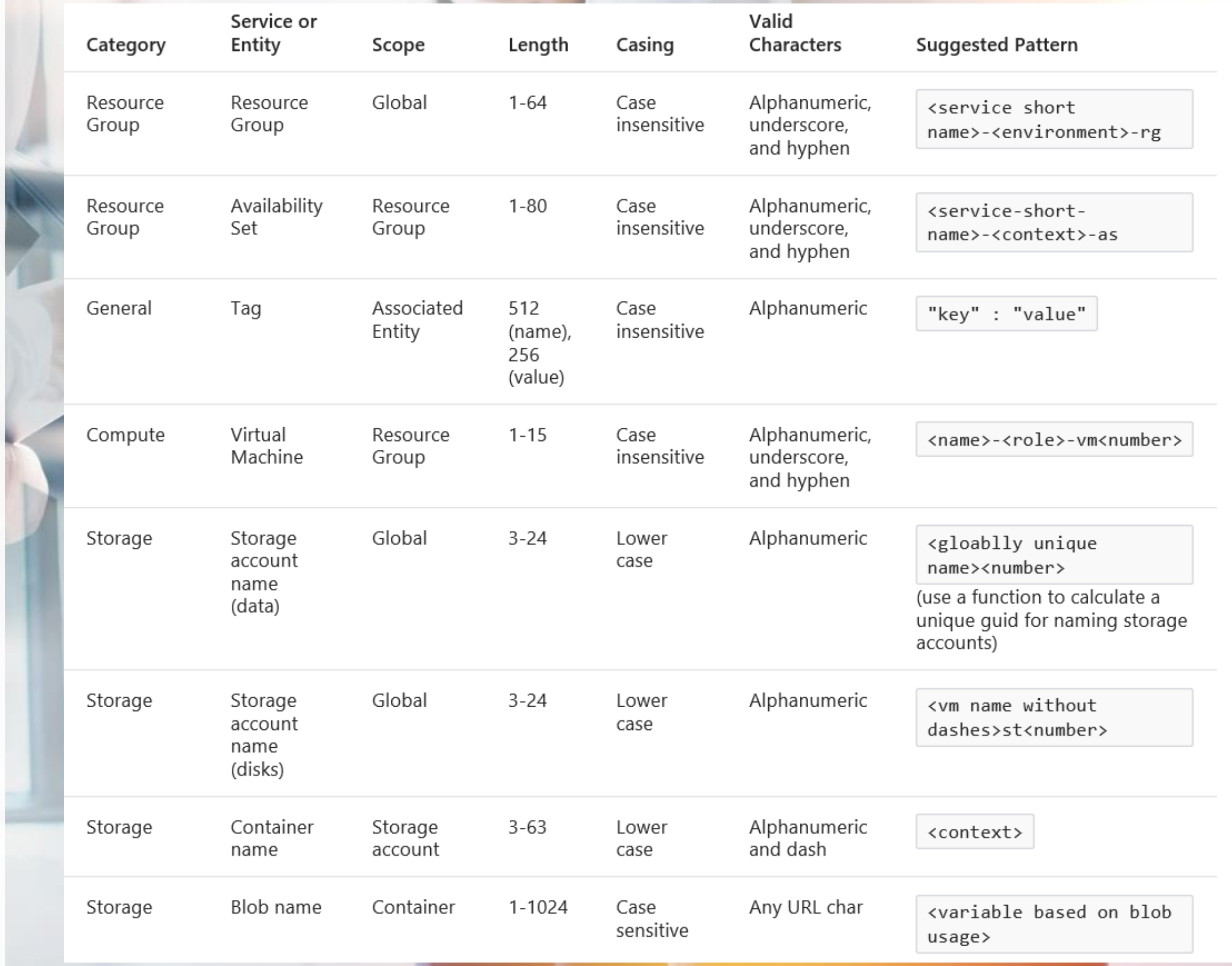
Naming Conventions

“Fear of a name increases fear of the thing itself.”

- J. K. Rowling

Names

- All ressources require names
  - NIC
  - Public IP
  - NSG
  - …
- Naming conventions in Azure per resource
- Prefixes or suffixes help



Category	Service or Entity	Scope	Length	Casing	Valid Characters	Suggested Pattern
Resource Group	Resource Group	Global	1-64	Case insensitive	Alphanumeric, underscore, and hyphen	`<service short name>-<environment>-rg`
Resource Group	Availability Set	Resource Group	1-80	Case insensitive	Alphanumeric, underscore, and hyphen	`<service-short-name>-<context>-as`
General	Tag	Associated Entity	512 (name), 256 (value)	Case insensitive	Alphanumeric	`"key" : "value"`
Compute	Virtual Machine	Resource Group	1-15	Case insensitive	Alphanumeric, underscore, and hyphen	`<name>-<role>-vm<number>`
Storage	Storage account name (data)	Global	3-24	Lower case	Alphanumeric	`<gloablly unique name><number>` (use a function to calculate a unique guid for naming storage accounts)
Storage	Storage account name (disks)	Global	3-24	Lower case	Alphanumeric	`<vm name without dashes>st<number>`
Storage	Container name	Storage account	3-63	Lower case	Alphanumeric and dash	`<context>`
Storage	Blob name	Container	1-1024	Case sensitive	Any URL char	`<variable based on blob usage>`

Azure Governance

Employee Organizational Change and Operations

- Transformation of organization, tied to DevOps
  - Increased **multi-skill** frameworks
  - Emphasis on **code, repeatability, automation**

Traditional IT Organization

Windows Team

Linux Team

Storage Team

Network Team

Security Team

Management Team

Virtualization Team

Identity Team

ITSM Automation Team

Business Unit Application Teams

Architecture Team

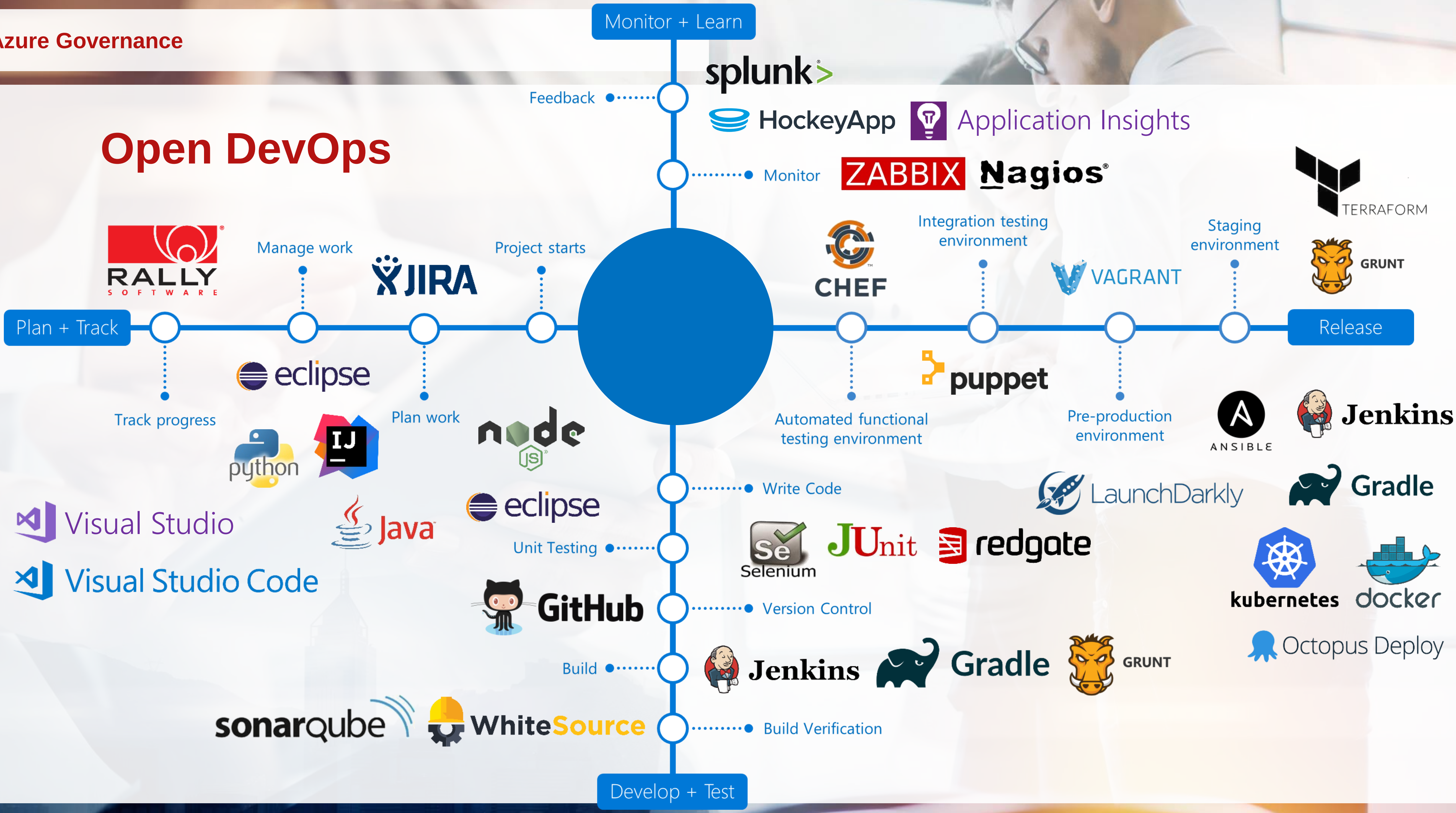
Modern IT Organization

Corporate Cloud Architecture & Operations

Application DevOps Teams

Security

Open DevOps



Monitor + Learn

Feedback

splunk>

HockeyApp

Application Insights

Monitor

ZABBIX

Nagios

TERRAFORM

Plan + Track

RALLY SOFTWARE

Manage work

JIRA

Project starts

Track progress

eclipse

Plan work

python

IJ

node JS

eclipse

Java

Visual Studio

Visual Studio Code

CHEF

Integration testing environment

VAGRANT

Staging environment

GRUNT

Release

puppet

Automated functional testing environment

Pre-production environment

ANSIBLE

Jenkins

Write Code

LaunchDarkly

Gradle

Unit Testing

Se Selenium

JUnit

redgate

kubernetes

docker

GitHub

Version Control

Build

Jenkins

Gradle

GRUNT

Octopus Deploy

sonarqube

WhiteSource

Build Verification

Develop + Test