



# Why you need rules to get into the cloud...

## ...and how to define them

Eric Berg | COMPAREX AG






# Eric Berg

 Lead IT-Architekt – Team Azure / Team Modern Workplace

 Azure, Datacenter and Modern Workplace

 Azure, System Center, Windows Server and Client

 [info@ericberg.de](mailto:info@ericberg.de)

 [@ericberg\\_de](https://twitter.com/ericberg_de) | [@GeekZeugs](https://twitter.com/GeekZeugs)

 [www.ericberg.de](http://www.ericberg.de) | [www.geekzeugs.de](http://www.geekzeugs.de)





Thank you, sponsors!

**DATA ONE**

**Alegri**



Nigel Frank  
International

The Global Leader in Microsoft Recruitment

**arvato**  
BERTELSMANN



Azure Saturday 2018



## Why moving to the cloud?

“Here we are, trapped in the amber of the moment. There is no why.”

- Kurt Vonnegut Jr.





Mainstream

Standards

Be More Agile

Continuous Development

Build Cloud-Born Apps

Automation

DevOps At ITs Best

Windows NT No Longer Supported

Innovation Leader

New Opportunities

Cost Savings

Require Less Employees

Individualize Everything

Host Off-Site

Large Scale



Azure Saturday 2018



# What is Cloud Governance?

“Learn the rules like a pro, so you can break them like an artist.”

- *Pablo Picasso*

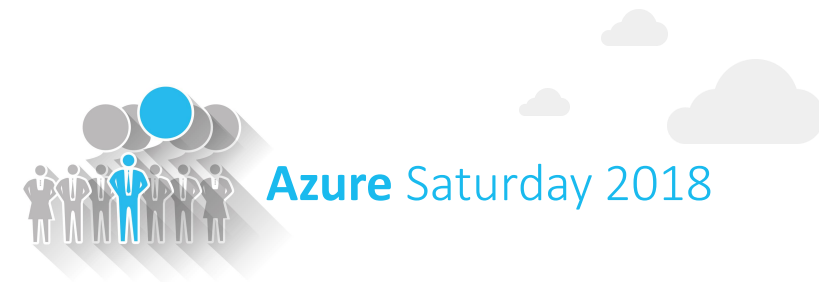




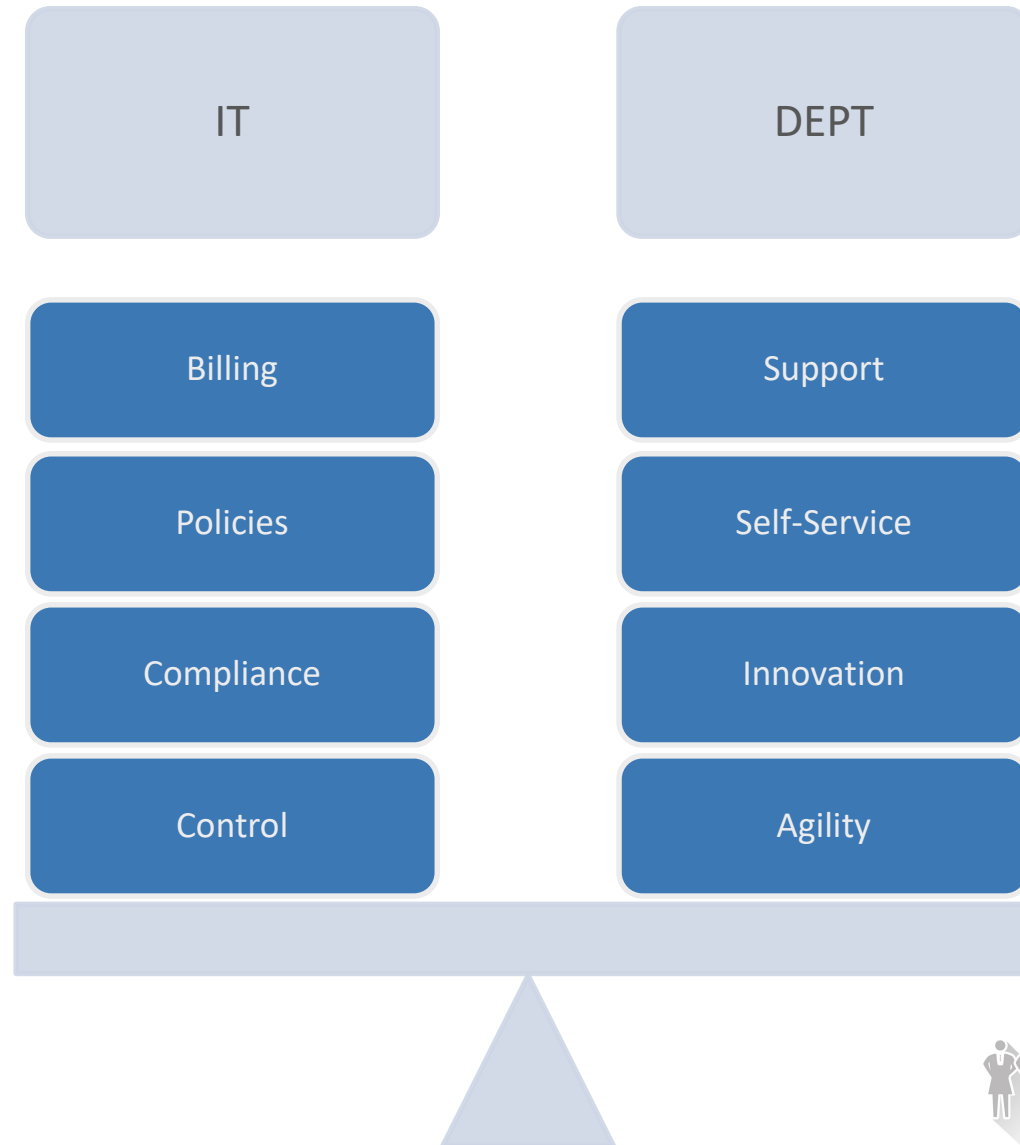
# Cloud Governance

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

Source: [www.businessdictionary.com](http://www.businessdictionary.com)

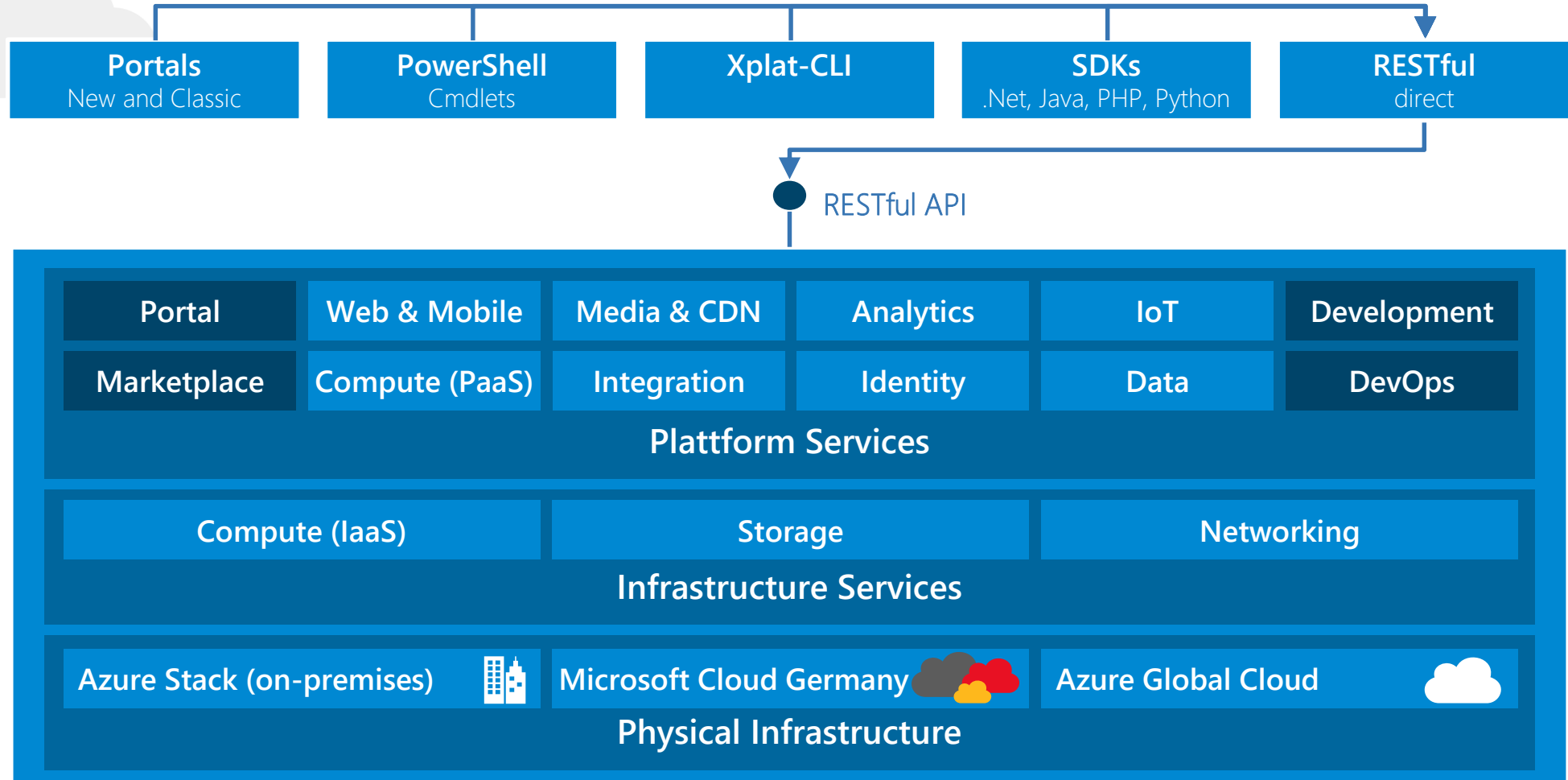


# Balancing needs





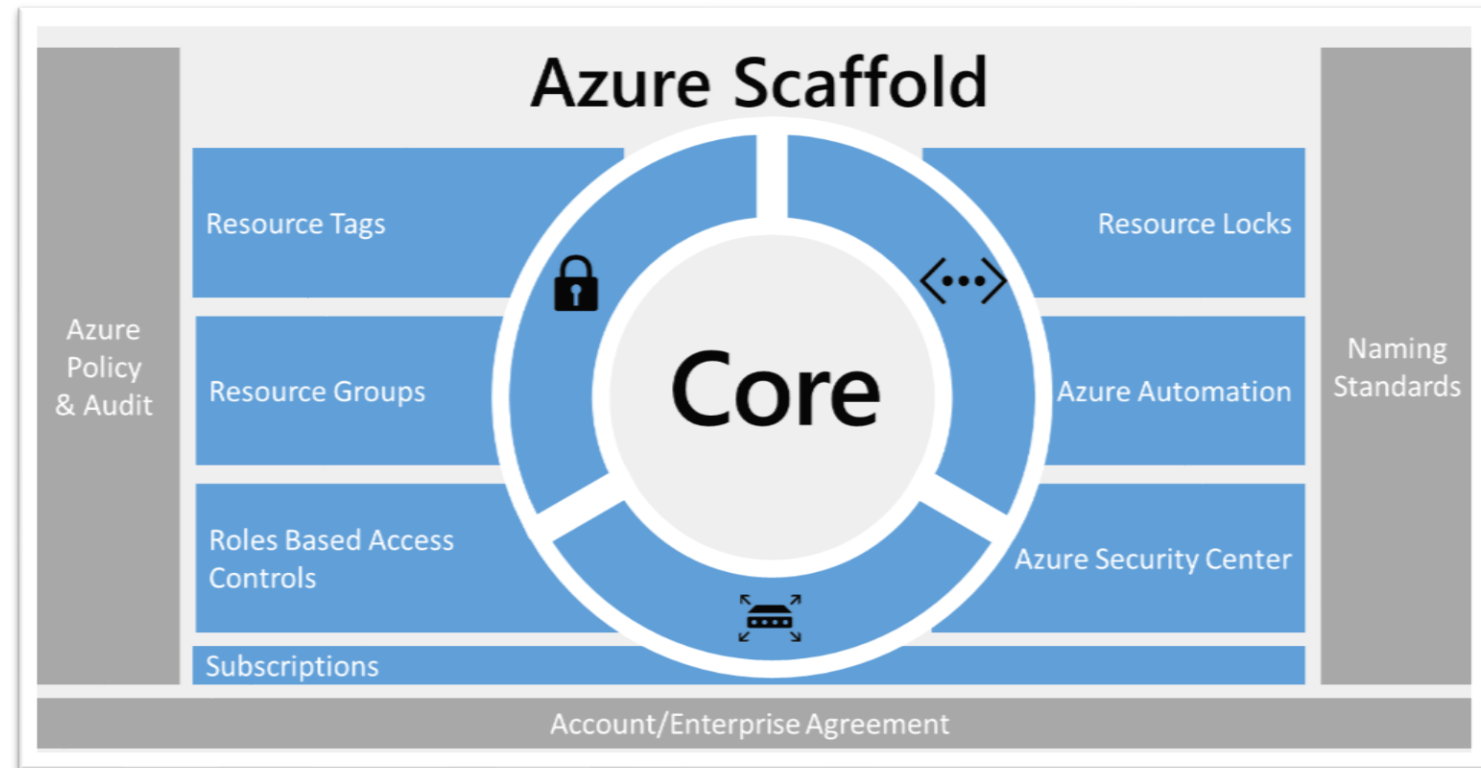
# Azure Management



# Azure Governance

„So it's not gonna be easy...”

- Billing?!
- User Rights?!
- Protection?!
- Standards?!
- Audits?!





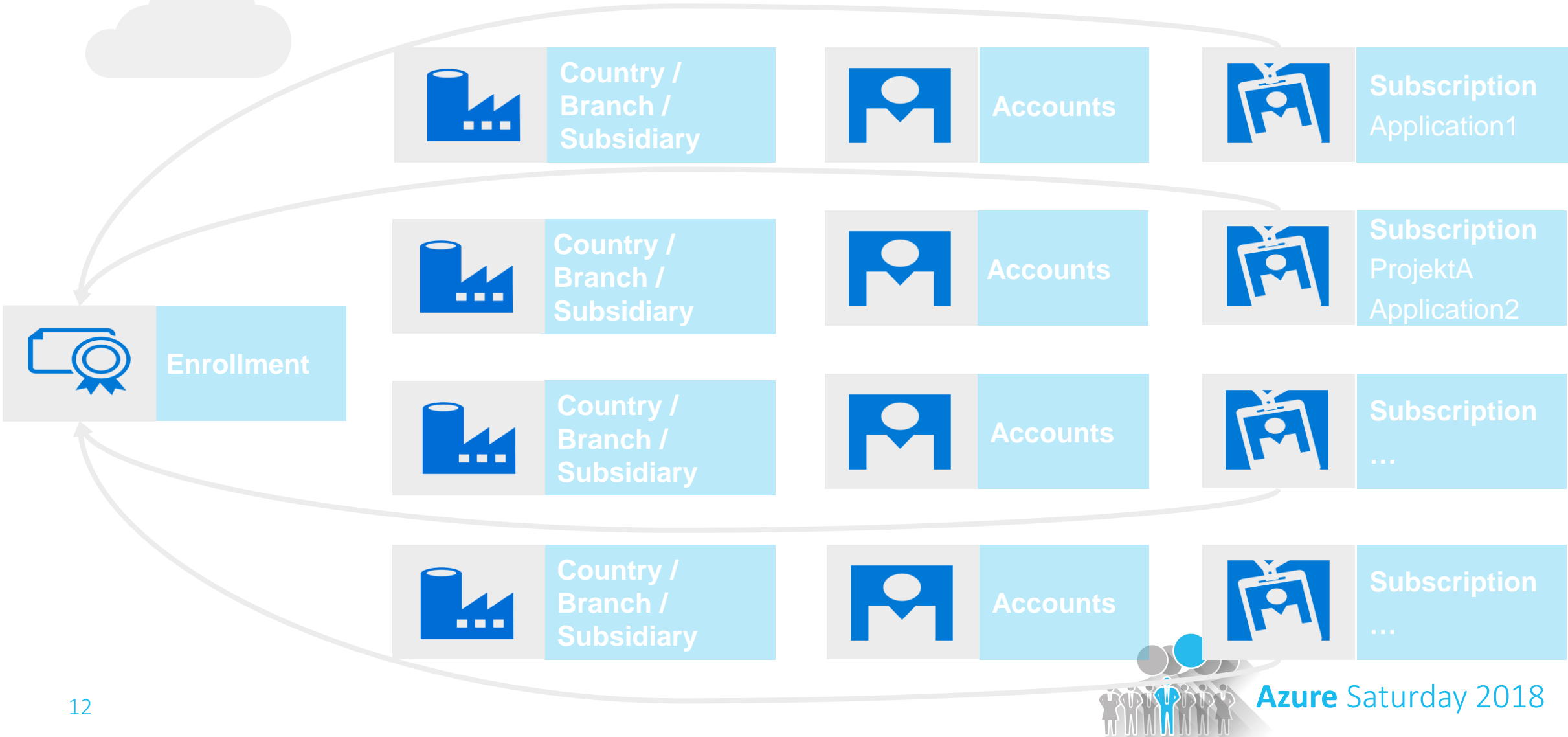
# Hierarchy

“Hierarchy works well in a stable environment.”

- Mary Douglas



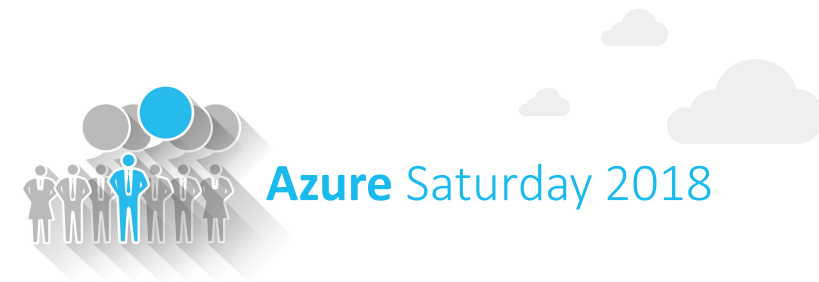
# Hierarchy



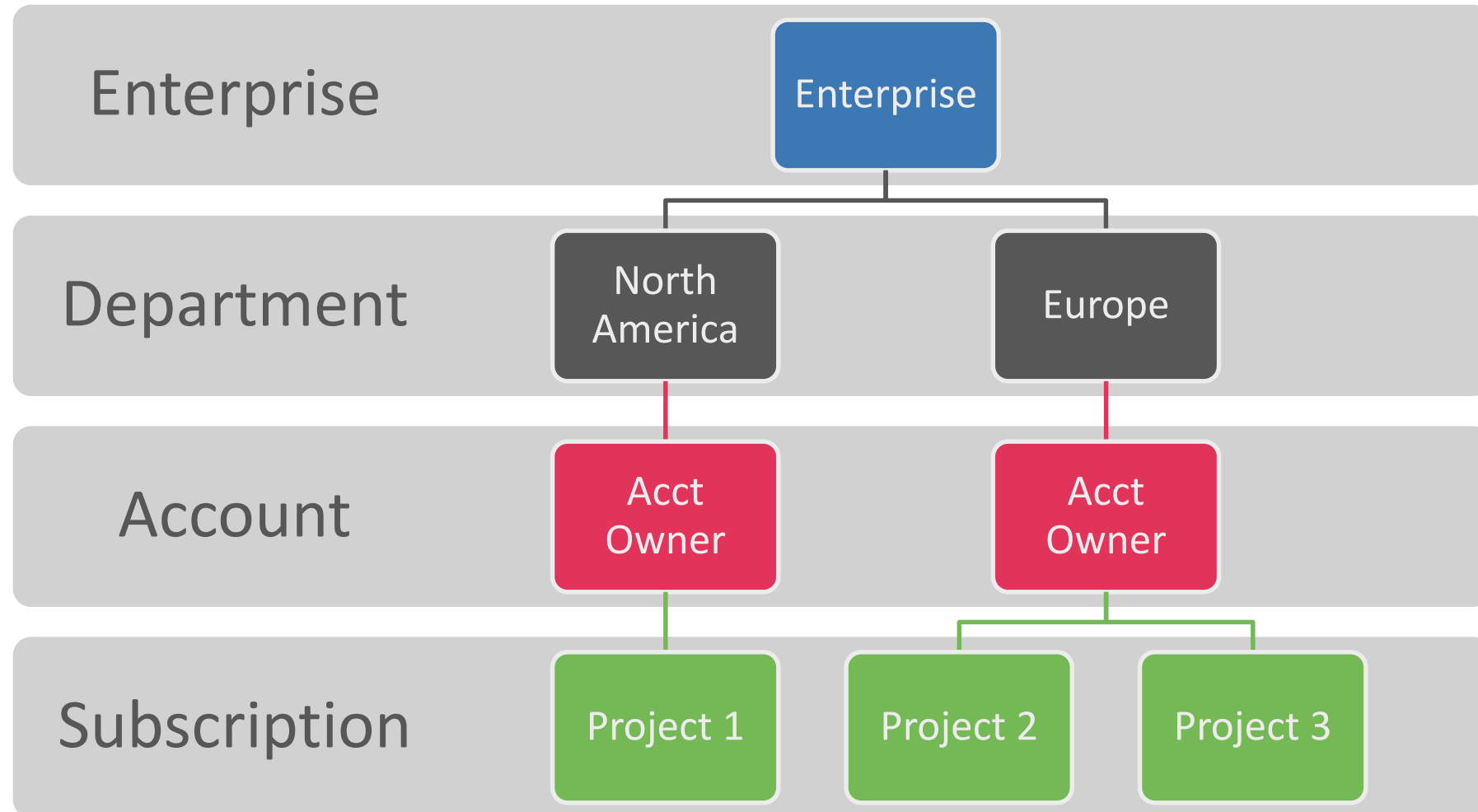


# Hierarchy Components

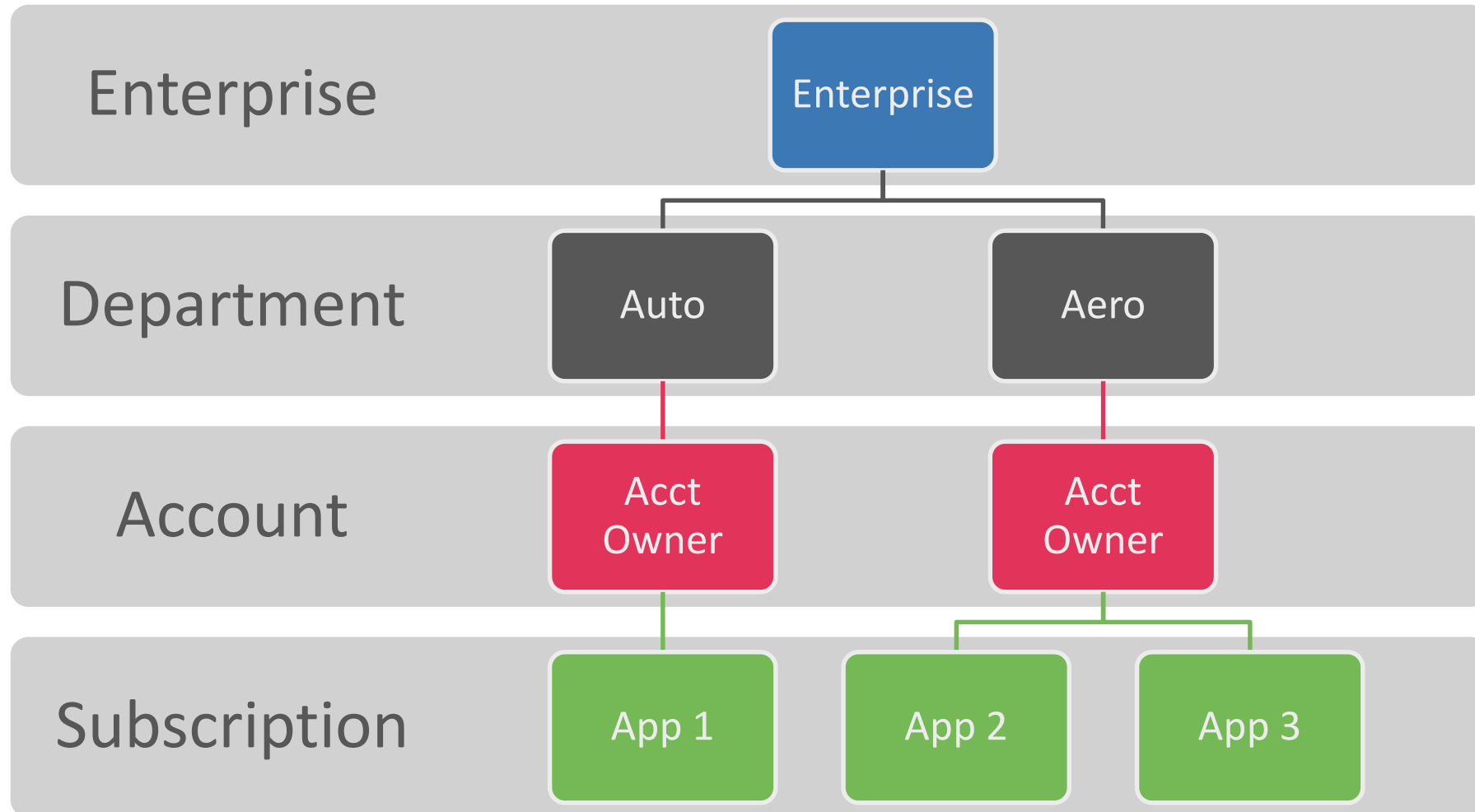
- Enrollment
  - Contract and Billing
- Department
  - Logical Unit with Owner
- Account
  - User Account with the ability to have subscriptions
- Subscription
  - Virtual Datacenter – where the magic happens



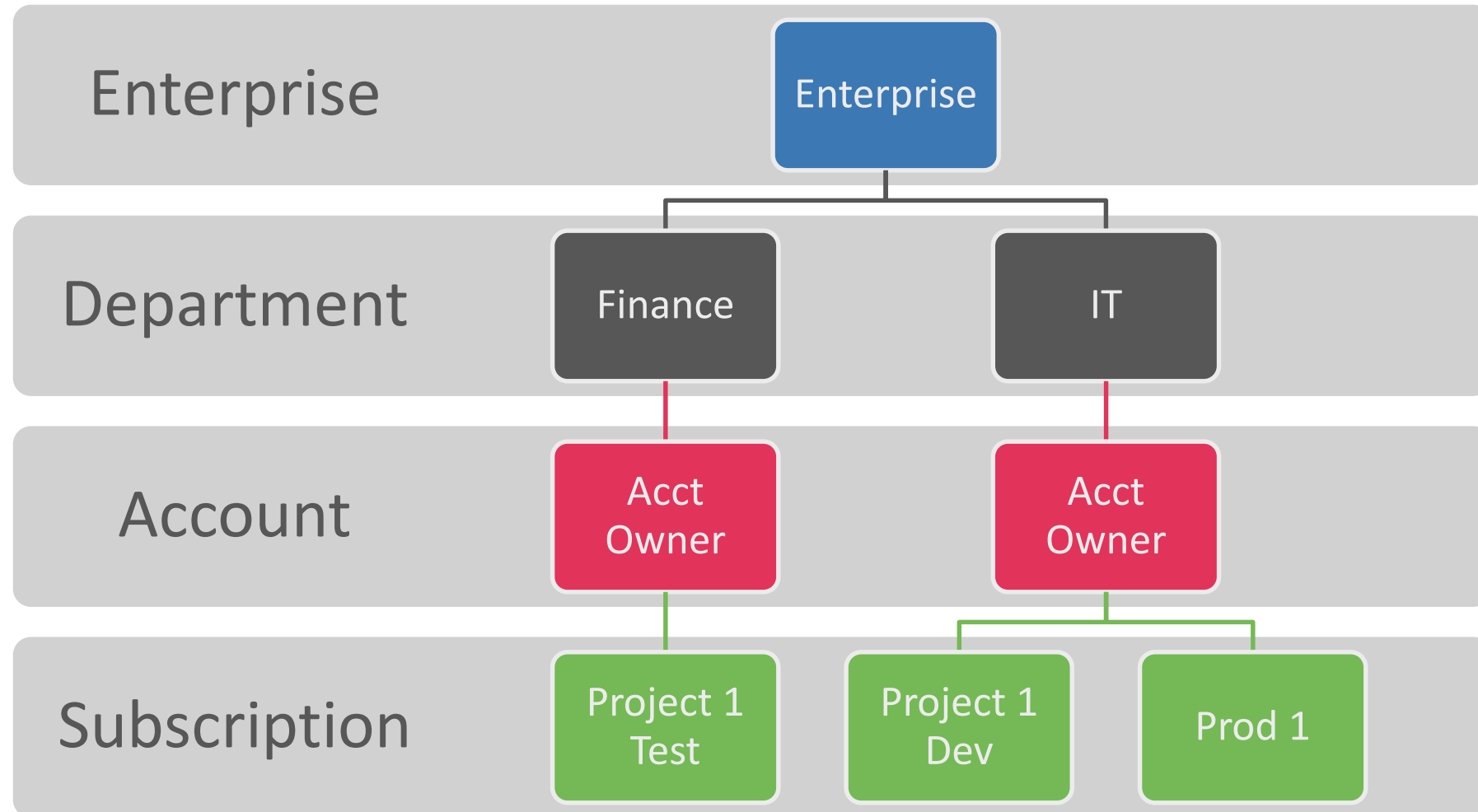
# Hierarchy - Geographic



# Hierarchy - Division



# Hierarchy - Function







## Resource Group

“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

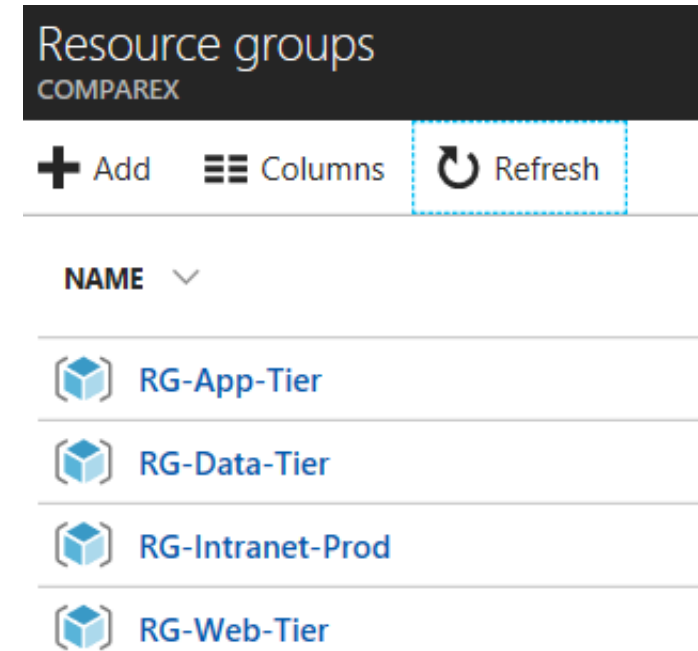
West Europe

▼



# Resource Group

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





## Resource Tags



# Resource Tags

- Billing in Azure difficult
- List of resource cost

[illegible]

# Resource Tags

- Property : Value
- Tags help to assign cost / responsibility
- Always tag RGs
  - Owner
  - Department
  - Environment
- Other resources as required
- Tags are your friends!
- Define tags in advance!
- Tag in Template!





## Resource Locks

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

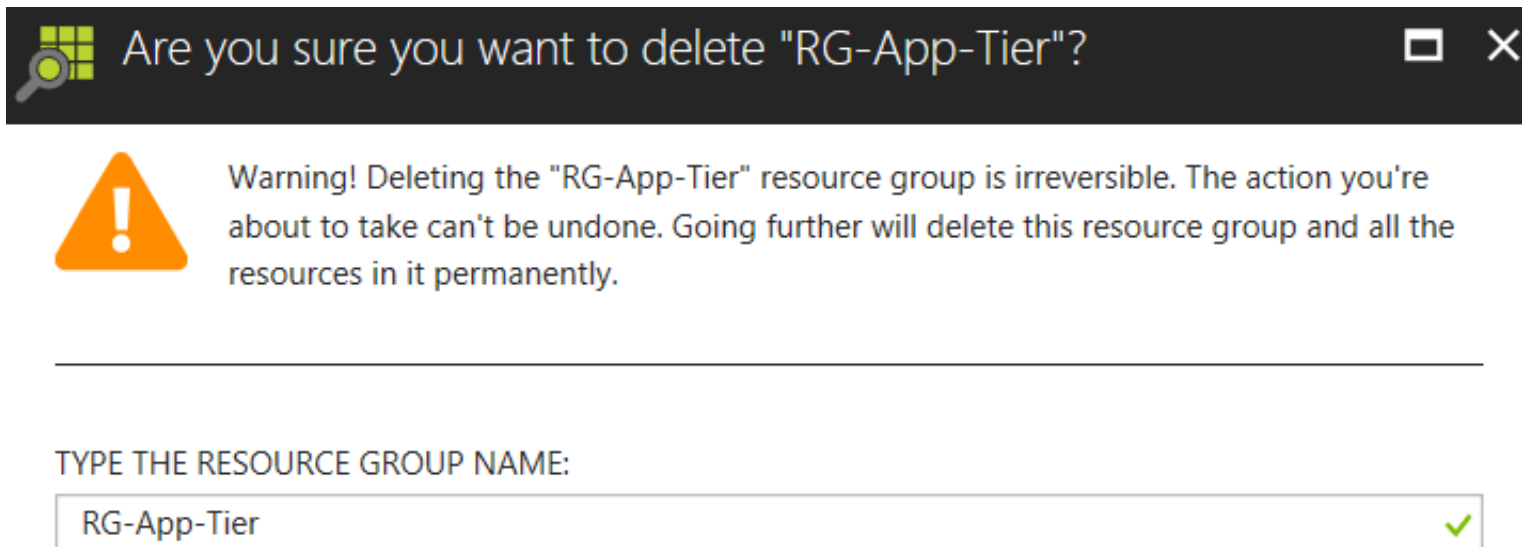
*- Julia Hoban*






# 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-App-Tier"?

 Warning! Deleting the "RG-App-Tier" 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.

---

TYPE THE RESOURCE GROUP NAME:

RG-App-Tier 



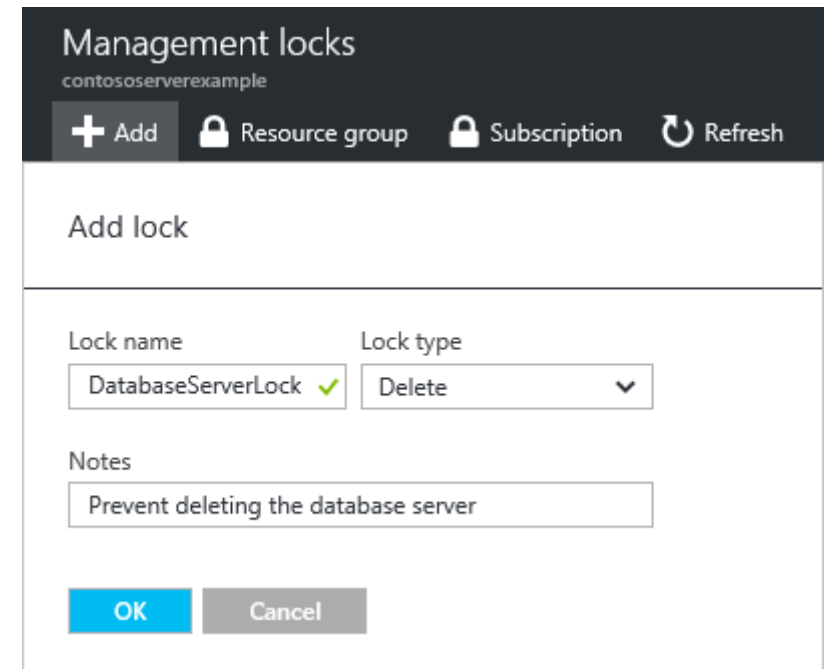


# Resource Locks

- 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!



The screenshot shows the 'Management locks' interface for 'contosoexample'. At the top, there are buttons for '+ Add', 'Resource group', 'Subscription', and 'Refresh'. Below this is a section titled 'Add lock'. It contains two input fields: 'Lock name' with the value 'DatabaseServerLock' and a green checkmark, and 'Lock type' with a dropdown menu showing 'Delete'. Below these is a 'Notes' section with a text area containing 'Prevent deleting the database server'. At the bottom are 'OK' and 'Cancel' buttons.



## Resource Policies

“You are remembered for the rules you break.”

- Douglas MacArthur





# Resource Policies

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

Learn more'. Below this is a section titled '\* Policy definition' with a list of policy types: 'Allowed locations', 'Allowed resource types', 'Allowed storage account SKUs', 'Allowed virtual machine SKUs', 'Not allowed resource types', and 'Require SQL Server version 12.0'. A scroll bar is visible on the right of the list." data-bbox="550 450 950 839"/>



# Resource Policies

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

Add assignment  
PREVIEW

Policies can be assigned to subscriptions and resource groups. Fill in the below fields to create a new assignment for a policy [Learn more](#)

\* Policy ⓘ

Enforce tag and its value

▼

Enforces a required tag and its value.

\* tagName ⓘ

BillingTo

\* tagValue ⓘ

347600

\* Scope ⓘ

RG-App-Tier

▼

\* Display name ⓘ

Billing To Policy

✓

\* Id ⓘ

Billing To Policy

✓

28

Azure Saturday 2018



## Role-Based Access Control

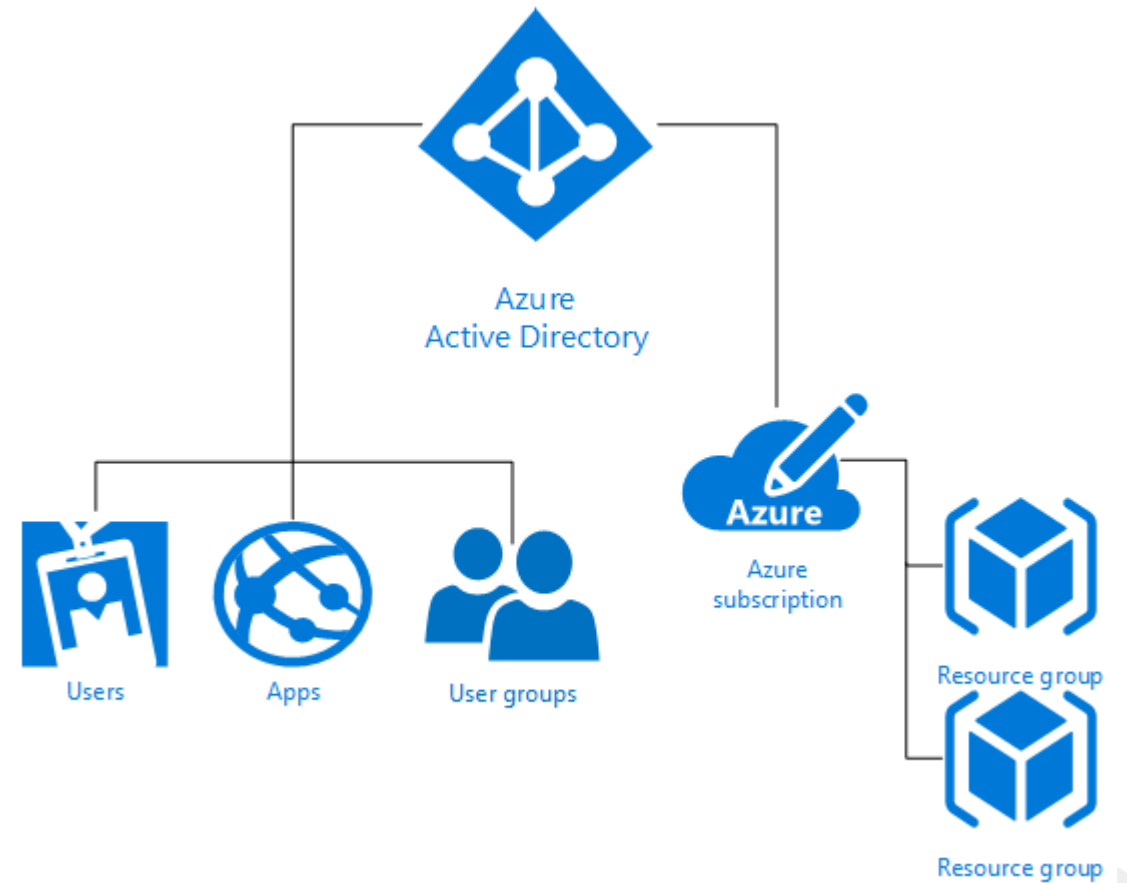
“Anything out there is vulnerable to attack given enough time and resources.”

- Kevin Mitnick



# RBAC

- Connection of Azure AD and Subscription
- Standard Roles
  - Owner
  - Contributor
  - Reader
- Extended Roles
  - Automation Operator
  - DevTest Labs User
  - ...
- Own Roles



# RBAC

- IAM can be set at all levels

RG-App-Tier - Access control (IAM)  
Resource group

Search (Ctrl+/)

Overview  
Activity log  
Access control (IAM)  
Tags

SETTINGS  
Quickstart  
Resource costs

+ Add Remove Roles

Name ⓘ  
Search by name or email

Group by ⓘ  
Role ▼

1 items (1 Users)

☐ NAME

OWNER

Berg, Eric  
Eric.Berg@comparex.cc

Add permissions

Role ⓘ  
Backup Operator

Select ⓘ  
norman.punge@comparex.com

Punge, Norman  
Norman.Punge@comparex.com





# Naming Conventions

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

- J. K. Rowling





# Names

- All resources 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	<code>&lt;service short name&gt;-&lt;environment&gt;-rg</code>
Resource Group	Availability Set	Resource Group	1-80	Case insensitive	Alphanumeric, underscore, and hyphen	<code>&lt;service-short-name&gt;-&lt;context&gt;-as</code>
General	Tag	Associated Entity	512 (name), 256 (value)	Case insensitive	Alphanumeric	<code>"key" : "value"</code>
Compute	Virtual Machine	Resource Group	1-15	Case insensitive	Alphanumeric, underscore, and hyphen	<code>&lt;name&gt;-&lt;role&gt;-vm&lt;number&gt;</code>
Storage	Storage account name (data)	Global	3-24	Lower case	Alphanumeric	<code>&lt;globally unique name&gt;&lt;number&gt;</code> (use a function to calculate a unique guid for naming storage accounts)
Storage	Storage account name (disks)	Global	3-24	Lower case	Alphanumeric	<code>&lt;vm name without dashes&gt;st&lt;number&gt;</code>
Storage	Container name	Storage account	3-63	Lower case	Alphanumeric and dash	<code>&lt;context&gt;</code>
Storage	Blob name	Container	1-1024	Case sensitive	Any URL char	<code>&lt;variable based on blob usage&gt;</code>





## 10 Tipps



# 10 Tipps for Azure

**Azure Governance**

**RBAC with care**

**Use premium  
managed disks**

**Never forget the  
firewall**

**Backup**

**Think about  
hidden cost**



# 10 Tipps for Azure

**Check 3rd Party  
licenses**

**Bandwith /  
Latency**

**Right-Sizing**

**Open for  
innovation**





**Azure** Saturday 2018  
We appreciate your feedback!



<https://form.responster.com/FnCF0u>





**Azure** Saturday 2018  
Thank you!

