AzureDay
Poland
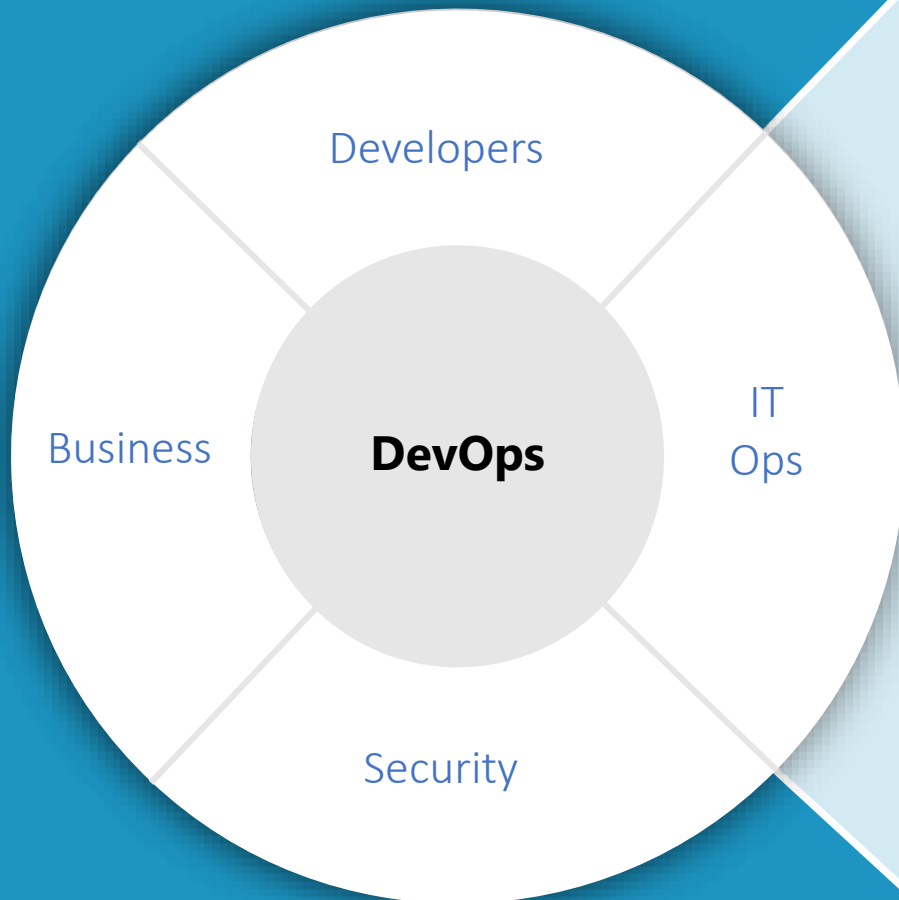
Explain the unknown - what are Azure Blueprints, Management Groups and Policies?!

Eric Berg | MVP Azure & CDM
Lead Architect Azure
COMPAREX AG | SoftwareONE

IT is transforming

DevOps

Developers

IT Ops

Business

Security

Adopting new cloud technologies

| ARM | Templates | Scripting | Functions | Event Grid |

Changing operating model

Developer Collaboration

Business value

Time to market

Azure Security & Management

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

NEW

Governance
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
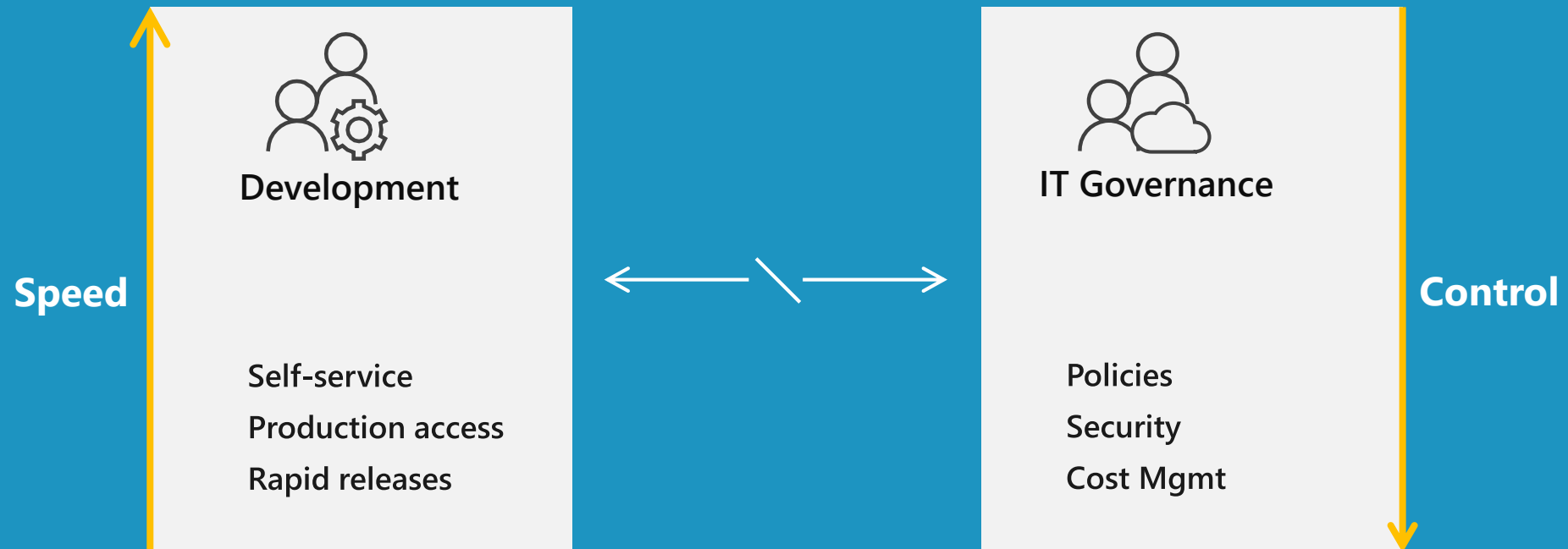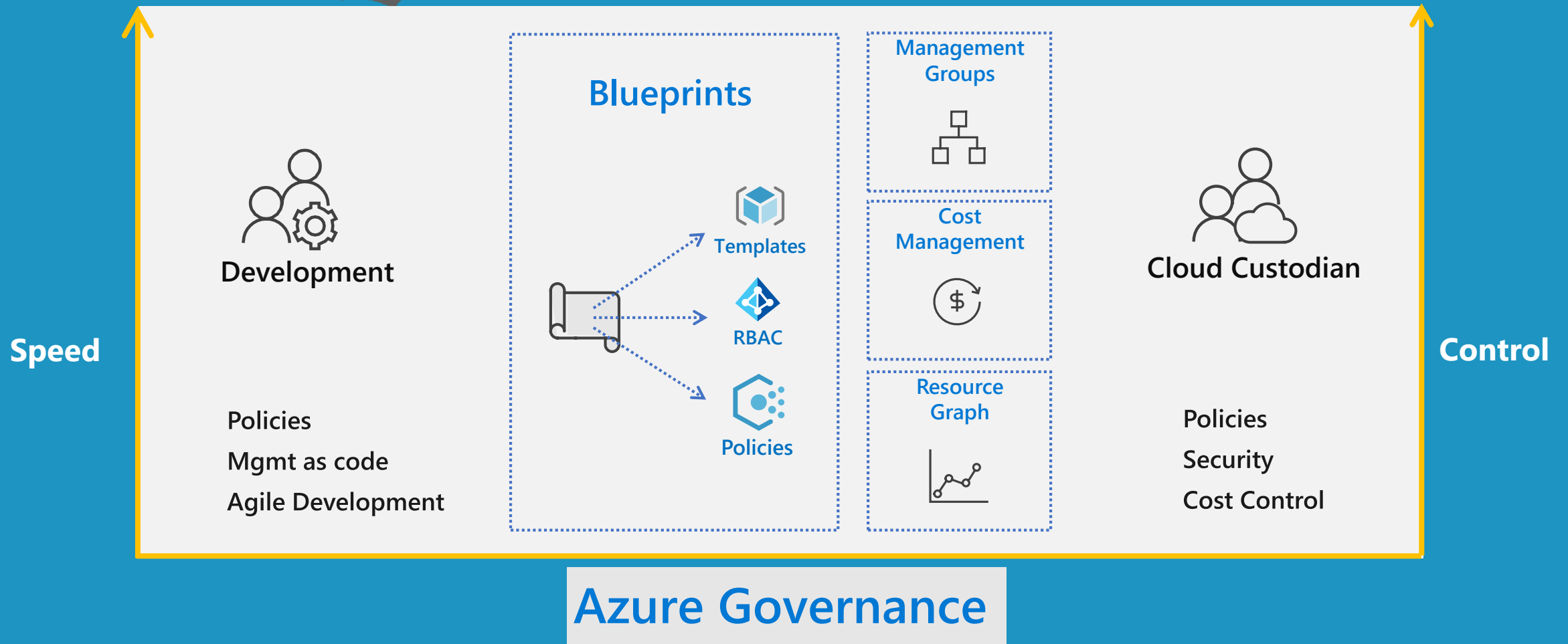Powerful scripting, configuration and update management

Governance in Azure

Built-in modern governance

Speed *and* control

Speed

Development

Policies

Mgmt as code

Agile Development

Blueprints

Templates

RBAC

Policies

Management Groups

Cost Management

Resource Graph

Cloud Custodian

Policies

Security

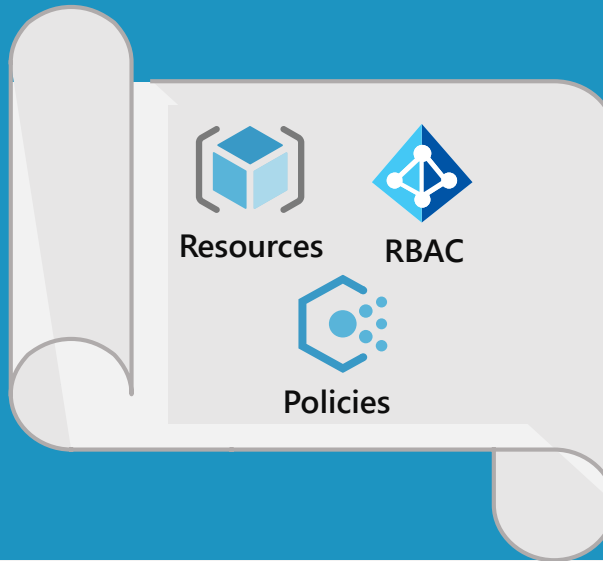Cost Control

Control

Azure Governance

Key Azure governance technologies

```
"policyRule": {
"if": {
"not": {
"field": "location",
"in":
"[parameters('listOfAllowedLocations
')]"
        }
    },
"then": {
"effect": "Deny"
        }
}
```
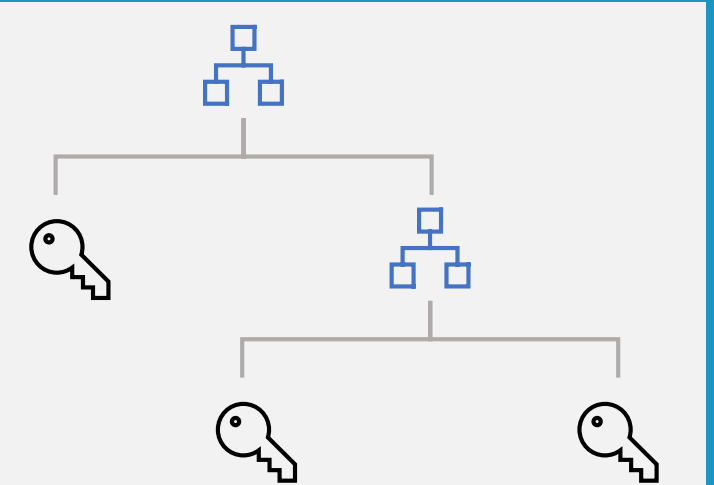
Resources   **RBAC**

Policies

Policy

Enforce or audit rules to ensure compliance.

Blueprints

Quickly create multiple subscriptions with resources, policies and users already setup.

Management groups

Map your organizational structure into Azure to enable governance in multi-tenant and cross-regional scenarios

Azure Resource Manager + Azure Resource Graph

Azure Management Groups

Introducing Azure Management Groups

Make environment management easier by grouping subscriptions together

- Grouping subscriptions into logical groups allow for new organization models

- Inheritance allows for single assignment of controls that apply to all subscriptions

- Aggregated views above the subscription level

Create a hierarchy of management groups that fit your organization

- Create a flexible hierarchy that can be updated quickly

- Hierarchy doesn't need to model the organizations billing hierarchy

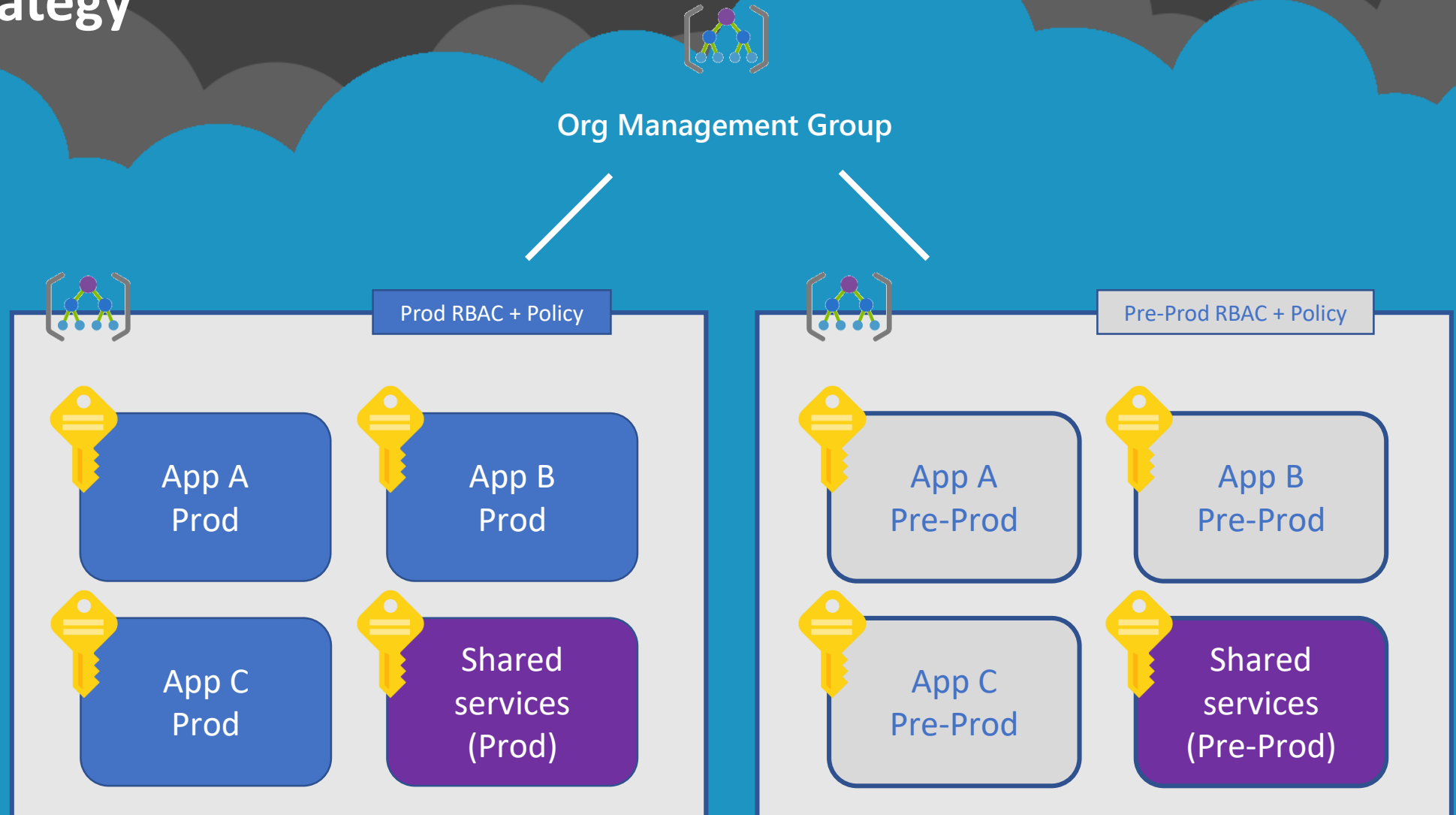- Can easily scale up or down depending on the organizational needs

Apply governance controls with policies and access controls along with other Azure services

- Azure Resource Manager (ARM) objects that allow integrations with other Azure services

- Azure services:
  - Azure Policy
  - RBAC
  - Azure Cost Management
  - Azure Blueprints
  - Azure Security Center

Management Group & Subscription Modeling Strategy

Org Management Group

Microsoft Recommended

Prod RBAC + Policy

| App A Prod | App B Prod |
| App C Prod | Shared services (Prod) |

Pre-Prod RBAC + Policy

| App A Pre-Prod | App B Pre-Prod |
| App C Pre-Prod | Shared services (Pre-Prod) |

Azure Policy

Azure Policy Journey

09/2017

Limited public preview

Introduced the new compliance engine (scans every 24 hours), UX and initiative

12/2017

Public preview

Introduced Management Group support

Compliance scan on resource change (delta scan)

Built-in definition support for remediation

05/2018

GA

Pricing details announcement (FREE!)

National clouds support

Introduced policy events view (count by user)

09/2018

Compliance percentage

Full fidelity of resources (store compliant resources)

'Last evaluated' timestamp

Trigger scan (on-demand scan) API

Custom definition support for remediation

Remediation on existing resources

'Denied due to policy' UX improvement

Progressive compliance results

In-guest Policy public preview

Default parameters

Azure DevOps integration

Azure Security Center integration

09/2017   **12/2017**   **05/2018**   **09/2018**

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

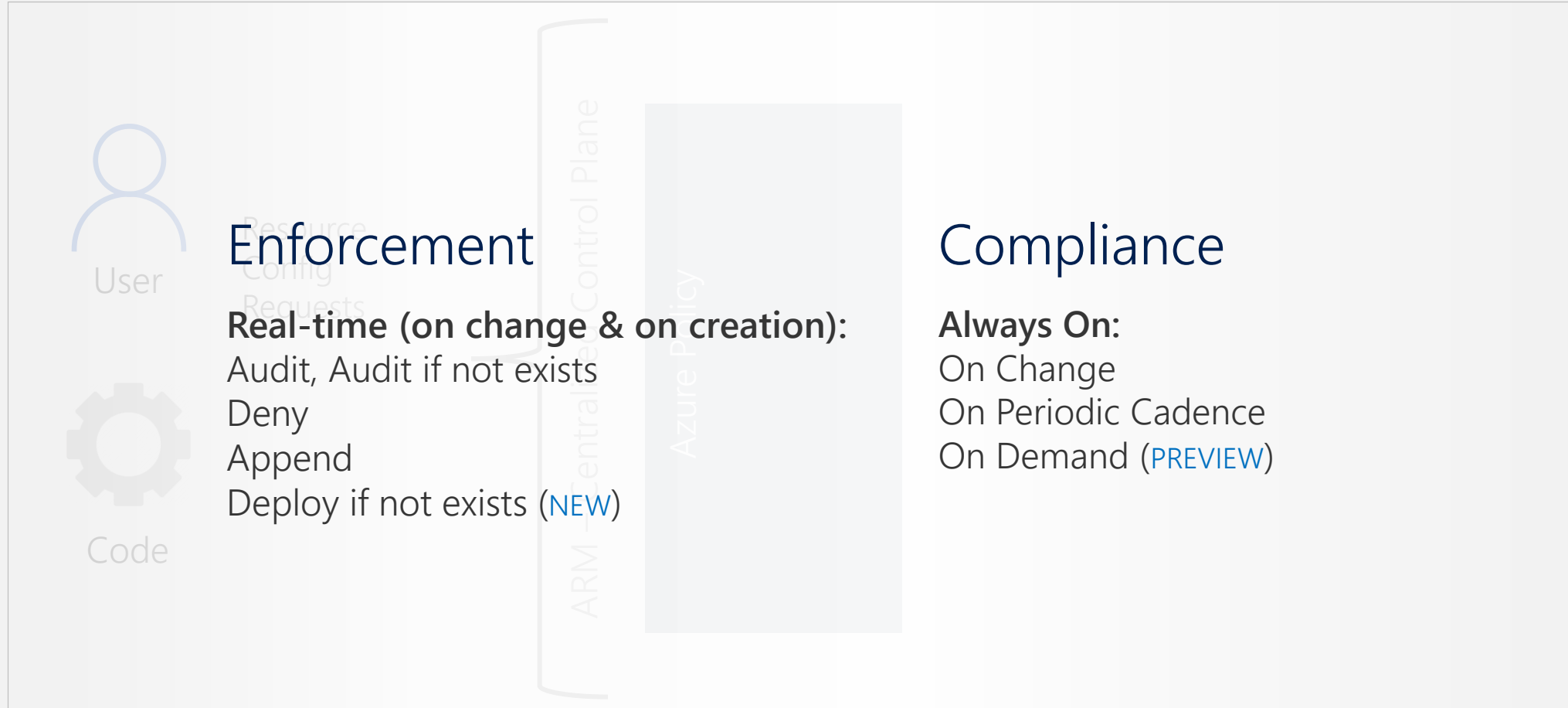- Real time remediation
- Remediation on existing resources (**NEW**)

Policy enforcement

How does it work?

User

Code

ARM – Centralized Control Plane

Azure Policy

Resource Config Requests

Enforcement

Real-time (on change & on creation):
Audit, Audit if not exists
Deny
Append
Deploy if not exists (NEW)

Compliance

Always On:
On Change
On Periodic Cadence
On Demand (PREVIEW)

How does it work?

How does it work?

User

Code

Resource Config Request

ARM – Centralized Control Plane
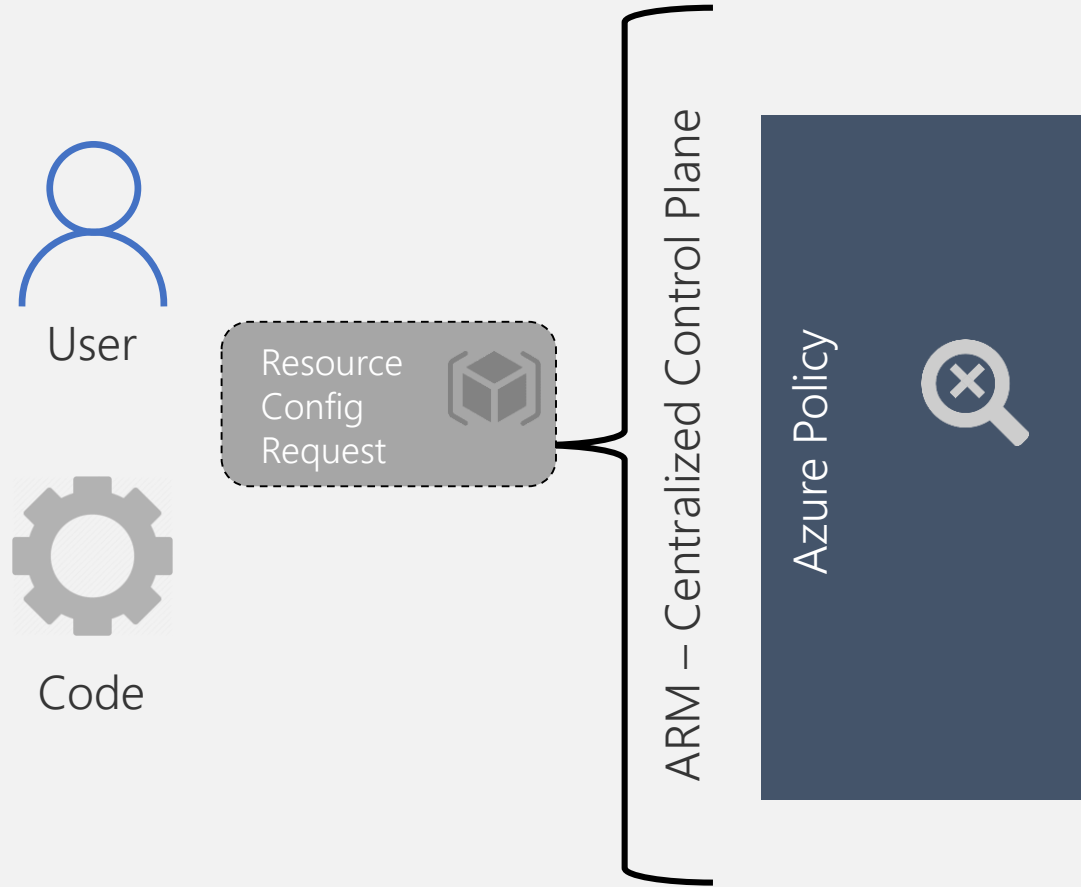
Azure Policy
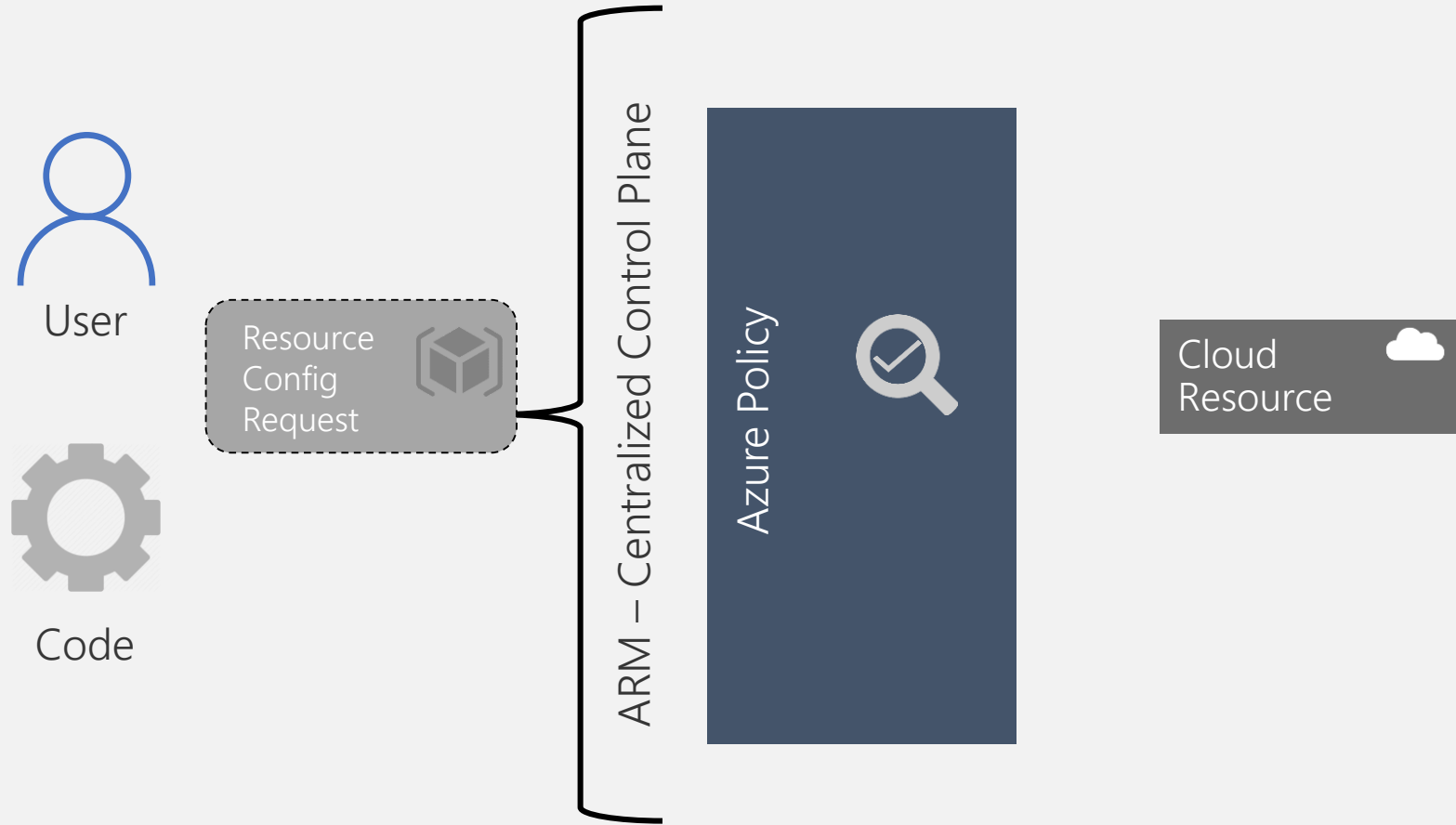
Cloud Resource
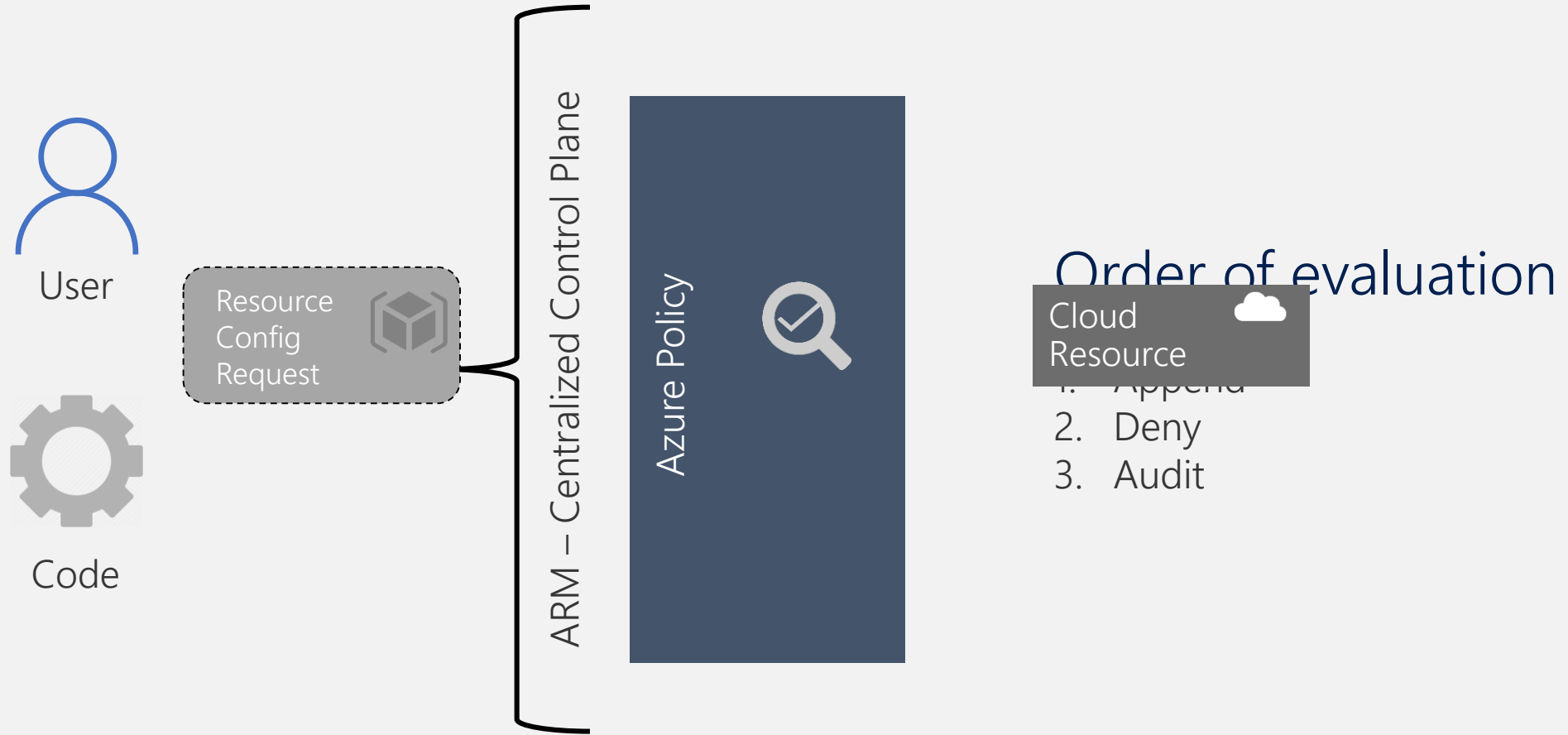
Order of evaluation

- Append
- Deny
- Audit
- DeployIfNotExists
- AuditIfNotExists

How does it work?

User

Code

Resource
Config
Request

ARM – Centralized Control Plane

Azure Policy

Order of evaluation

Cloud
Resource

1. Append
2. Deny
3. Audit

How does it work?

User

Code

ARM – Centralized Control Plane

Azure Policy

Cloud Resource

4. DeployIfNotExists
5. AuditIfNotExists

Policy limits

- 250 policy definitions per scope   Scope = Subsc or MgmtGroup
- 100 initiative definitions per scope
- 1000 policy set definitions per tenant
- 100 policy or initiative assignments per scope
- 20 Parameters per Policy Definition
- 100 Policies per Initiative Definition
- 100 Parameters per Initiative Definition
- 250 notScopes per Policy or Initiative Assignment
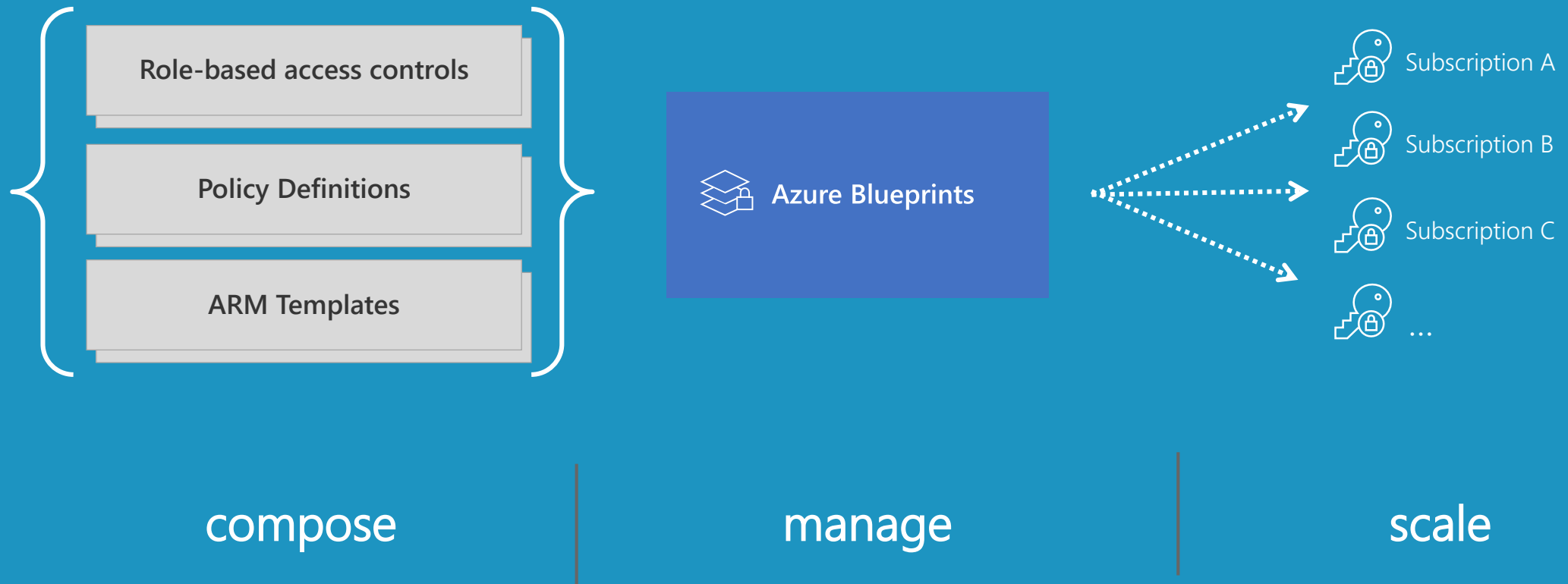- 512 Nested conditionals per Policy Rule

🏗️ Blueprints

Azure Blueprints

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

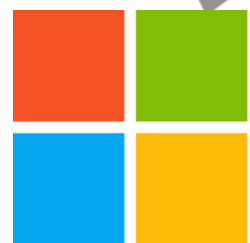| Role-based access controls |
| :---: |
| Policy Definitions |
| ARM Templates |

Azure Blueprints

Subscription A

Subscription B

Subscription C

...

compose   manage   scale

Demo

Azure Blueprints

Got questions?

Find me today... :-)