

# **Cloud Governance: Winning the battle between speed & control**

**Sonia Cuff**

**@SoniaCuff**

**Senior Cloud**

**Advocate Microsoft**



148,000  
0

A large, modern sign with a blue background and a prominent red diagonal band. On the red band, a white arrow points to the left, followed by the word "Emergency" in a bold, white, sans-serif font. The sign is positioned in front of a multi-story building with a grid of windows under a clear blue sky.

← Emergency

Startup with  
\$3M in assets  
files for bankruptcy

\$10 million penalties to  
be introduced for  
privacy law breaches

I feel the  
need, the  
need for  
speed!

Developer

Negative,  
Ghost  
Rider, the  
pattern is  
full.

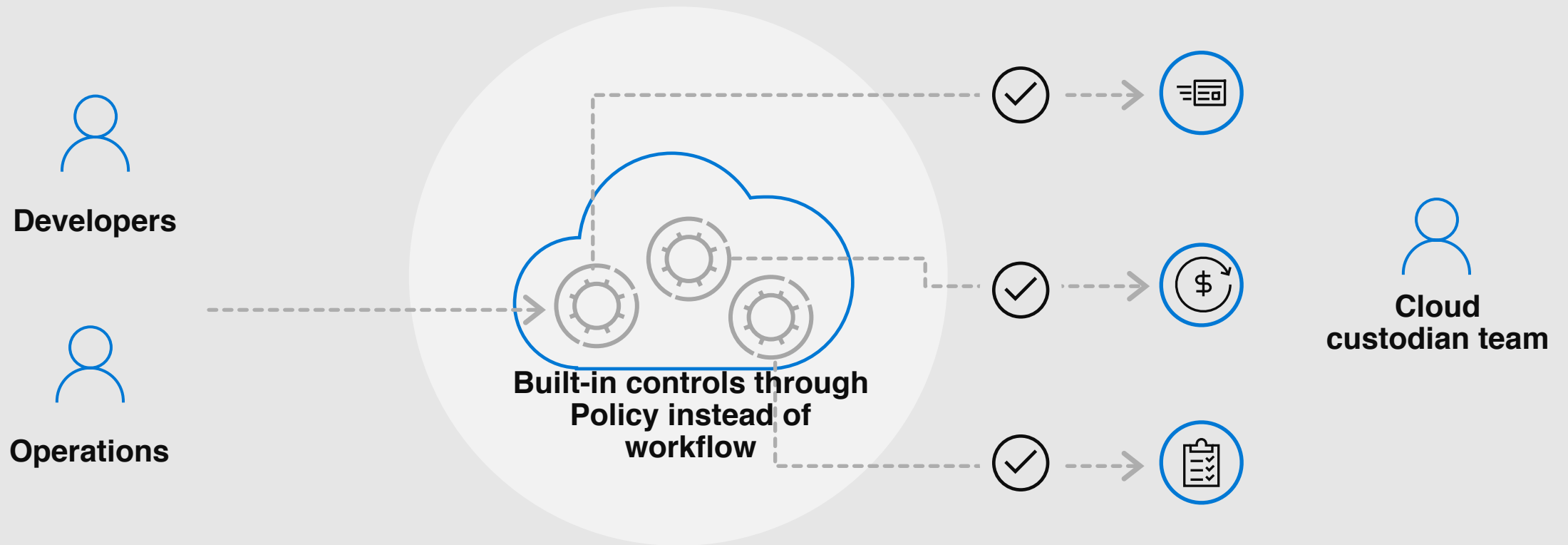
Sys



**Replace them with a machine!**

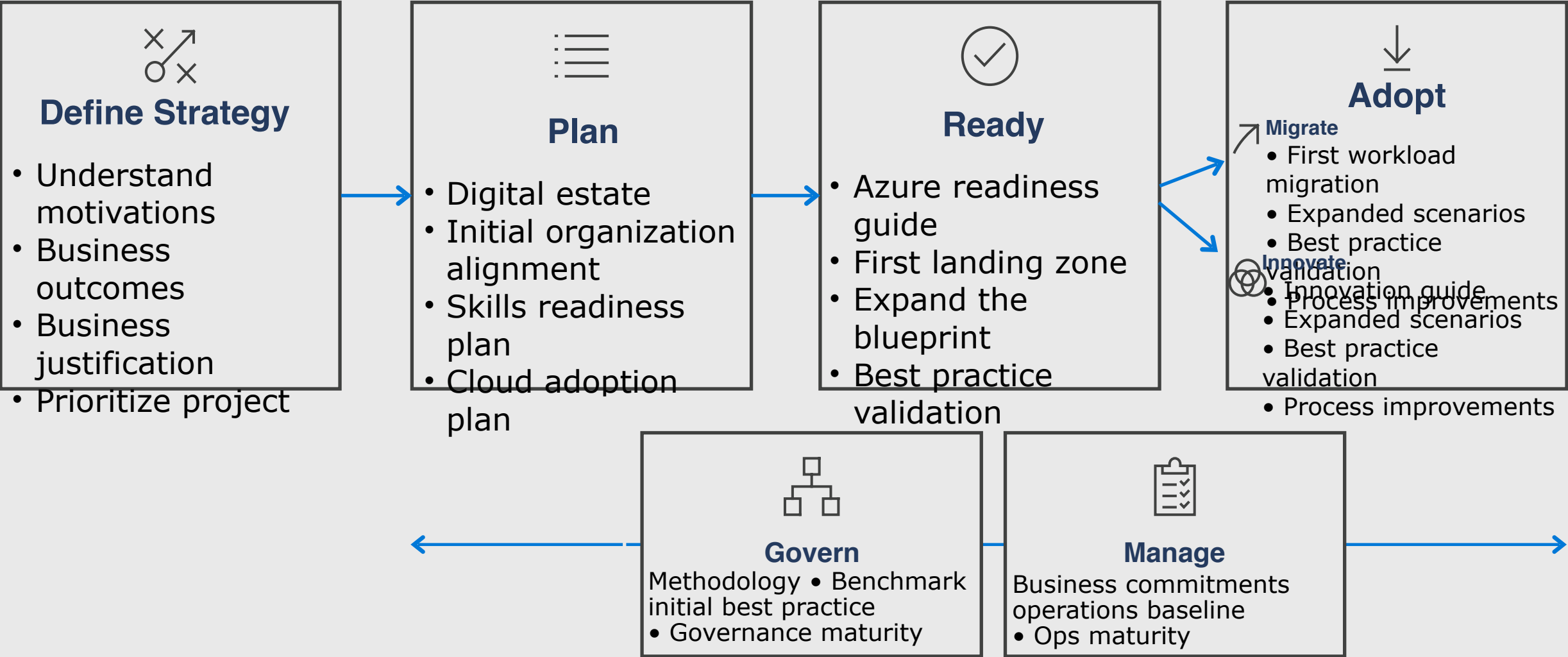


# Replace them with a machine!



**What goes into the machine?**

# Microsoft Cloud Adoption Framework – aka.ms/CAF



**What is Governance anyway?**

**Governance = Risk  
Management**

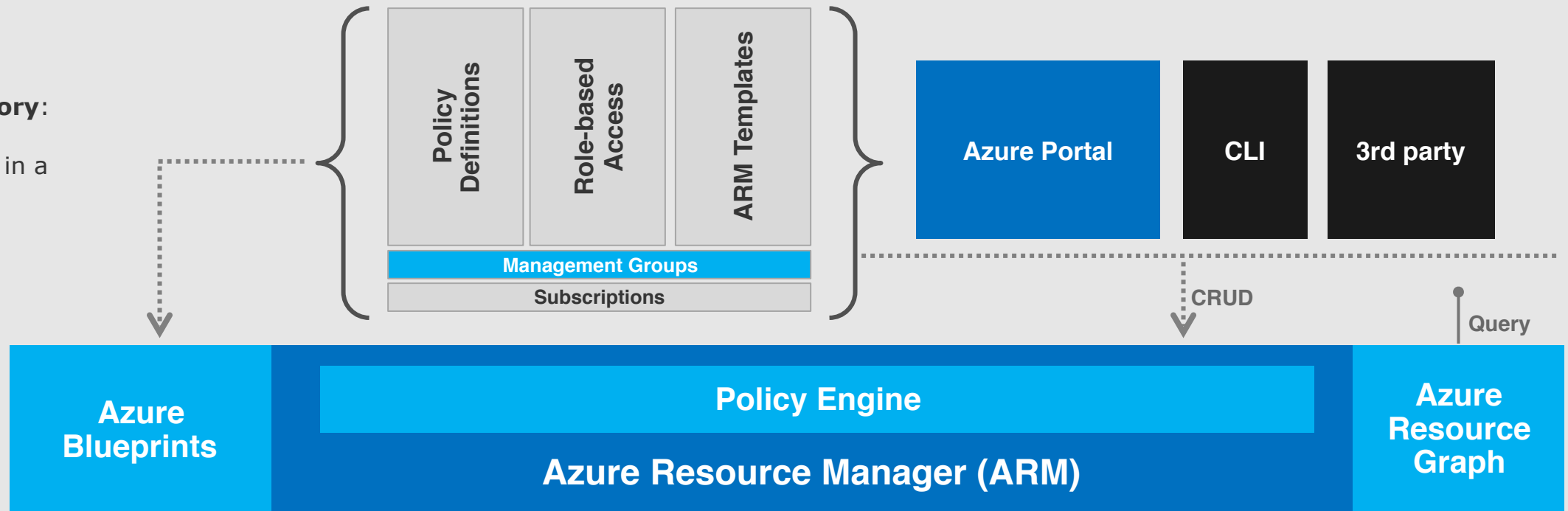
**Governance = Appropriate Safety  
Guardrails**

**Appropriate**

# Azure Governance Architecture

## 1. Environment Factory:

Deploy and update cloud environments in a repeatable manner



**2. Policy-based Control:** Real-time enforcement, compliance assessment and remediation at scale

**3. Resource Visibility:** Query, explore and analyze cloud resources at scale





# Business Risk



- ❑ Document evolving business risk

- ❑ Document risk tolerance, based on data classification & application criticality

# Business Risk Examples



# Policy & Compliance



- ❑ Convert risk decisions into policy statements

- ❑ Establish cloud adoption boundaries

# Policy Statement Examples



## 1. Cost Management

Expensive resources are blocked by default and require prior approval.

## 2. Security Baseline

No assets with a protected level of data may be deployed to the cloud, until sufficient requirements for security are approved and implemented (eg network, encryption, access rights).

## 3. Identity Baseline

All assets deployed to the cloud are controlled using approved

# Policy Statement Examples



## 4. Resource Consistency

SLA, performance and BC/DR requirements have been defined and resource configurations meet those requirements.

## 5. Deployment acceleration

All assets must be grouped and tagged according to the organisation's defined strategies.

# Security Baseline



❑ Compliance with IT Security requirements

❑ Apply security baseline to all adoption efforts

# Identity Baseline



- ❑ Enforce identity and access baseline

- ❑ Apply role definitions and assignments

- ❑ Monitor for key access changes

# Resource Consistency



Enforce consistency of new resources

Ensure discoverability of resource configuration changes

Remediate or approve resource configuration changes



# Deployment Acceleration..



- ❑ Remove reliance on manual deployment or configuration
- ❑ Templates & scripts are in source-controlled platforms
- ❑ Deployment polices are consistent across all environments

Baseline  
policies

App  
data risks

App  
access risks

Ensure  
deployment  
consistency

Enforce tag  
structure

Design  
decision  
impact  
on costs

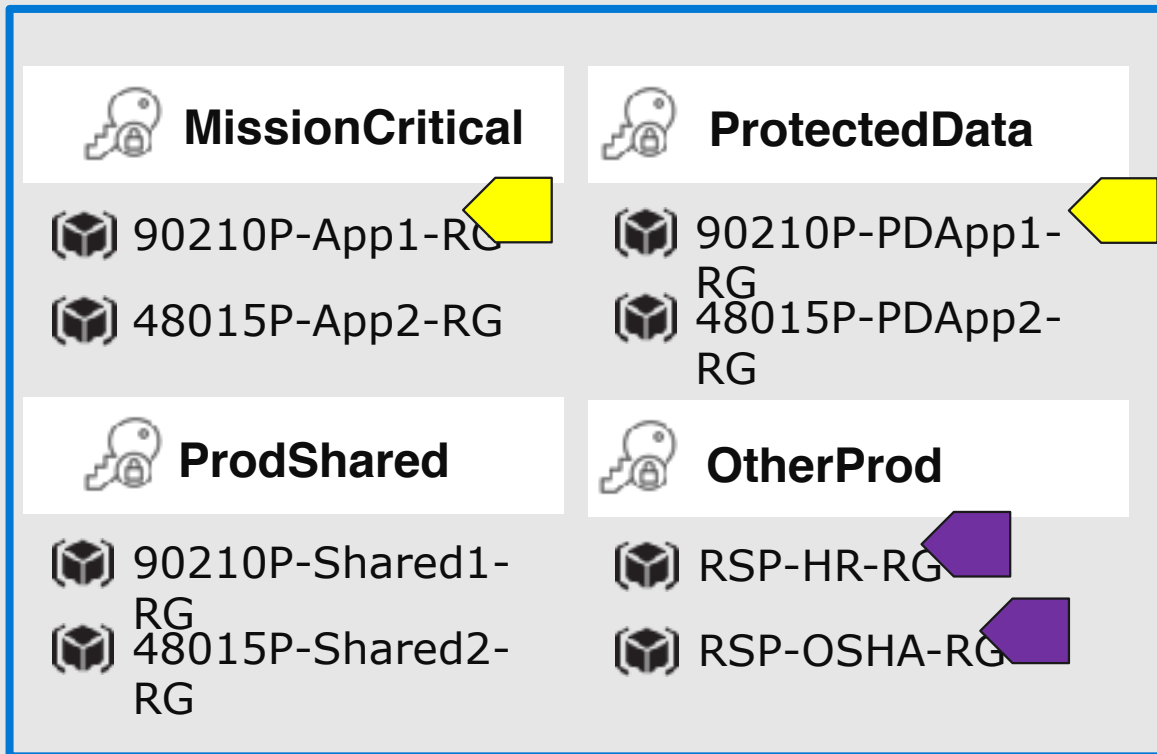
**Customer scenario**



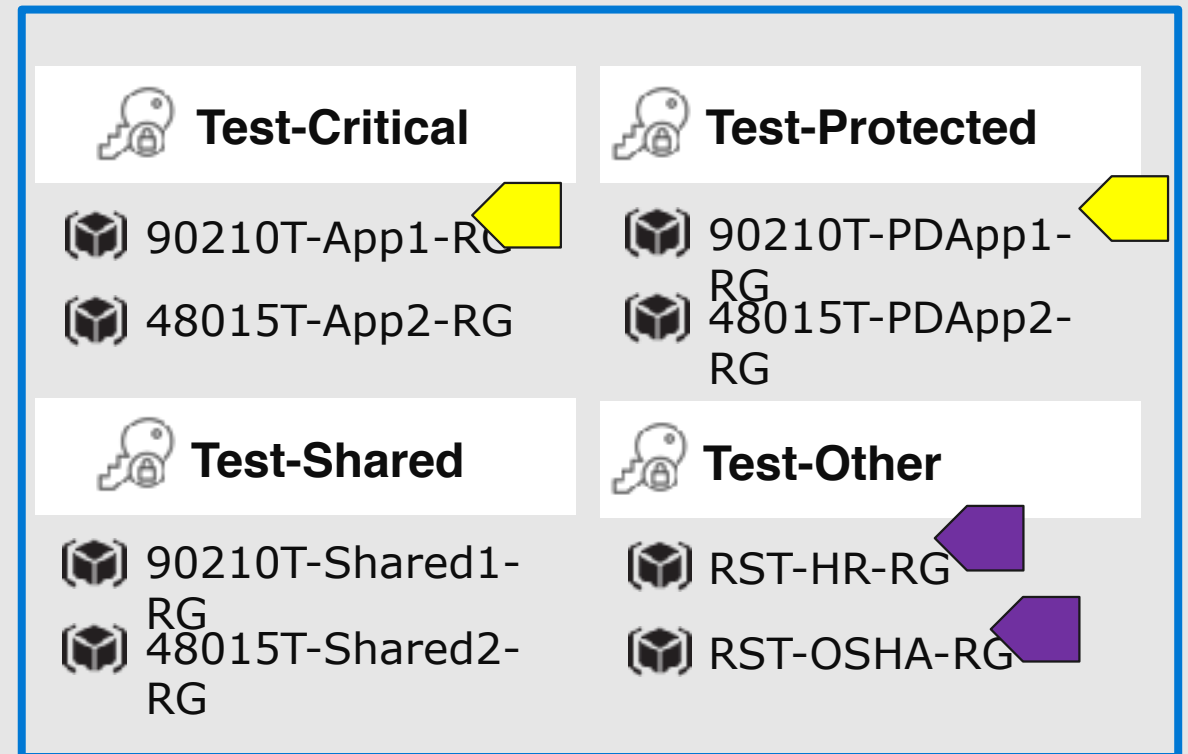
# Retail store applications



## Production




## Test



# Role Based Access Control



Cognitive  
Services Data  
Reader

Storage  
Account  
Contributor

Security  
Reader

Cost  
Management  
Reader

# Cost Management



Cloud



**Deadprogrammer**

@deadprogrammer

Follow



AWS is not about paying for what you use, it's about paying for what you forgot to turn off.

2:26 PM - 24 Apr 2019

3,234 Retweets

12,581 Likes



173



3.2K



13K



# Doing Cost Management Right

 **Estimating**

 **Managing**

 **Reviewing**



# Estimating cloud costs



# Cost Estimating – On-prem Virtual Machine

## Hardware

Chassis

Disk

RAM

CPUs

**Rack space**

- Licenses
  - Server OS
  - CALs

- Everything else
  - Electricity?
  - Labour?
  - Replacement parts?

# Cloud Cost Metering – Virtual Machines

**Compute Hours**

**IP Address Hours**

**Data Transfer In**

**Data Transfer Out**

**Standard Managed Disk**

**Standard Managed Disk Operations**

**Standard IO-Block Blob Read**

**Standard IO-Block Blob Write**

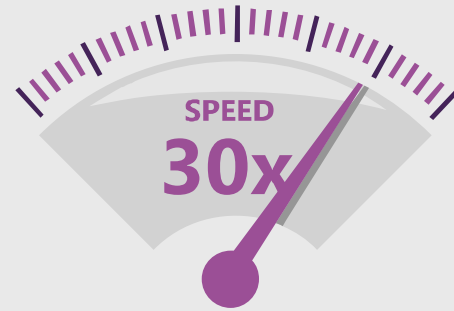
**Standard IO-Block Blob Delete**

- Region
- Tier
- Disk Type
- Traffic Zones
- Redundancy
- Licensing
- Subscription Agreement
- Reserved Instance

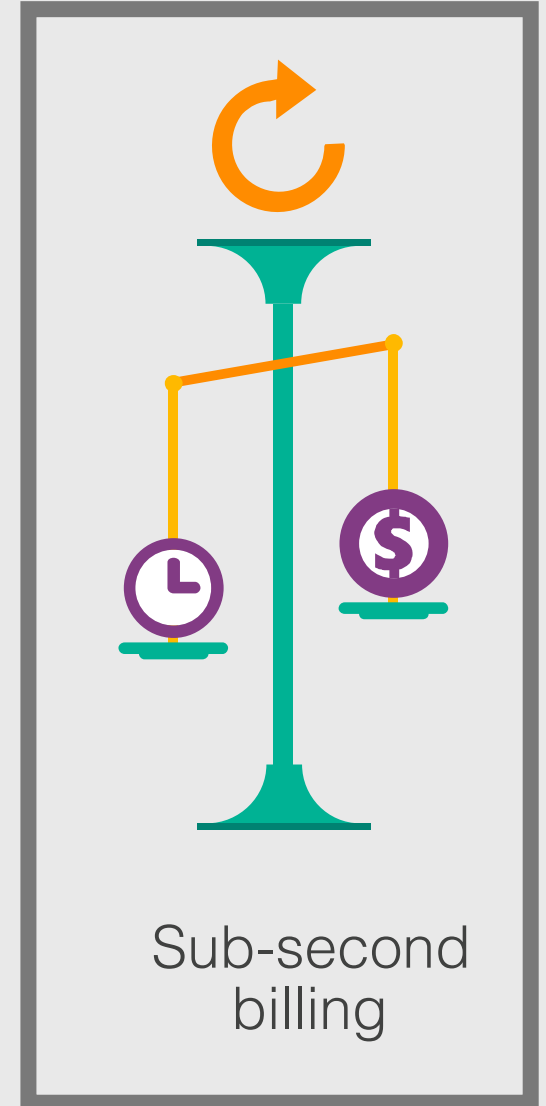
# Serverless



Abstraction  
of servers



Event-driven  
scale



Sub-second  
billing

**Design decisions have cost  
consequences**



# Design decisions

Managed disks

Storage tiers

Replication

Region

Traffic

# Purchasing options have cost consequences

Hard limit  
subscriptions

Dev/Test  
subscriptions

Enterprise  
Agreements  
v PAYG

1yr or 3yr  
commitment

# Demo – Pricing a solution



# Demo – Comparing Total Cost of Ownership



**Manage your Cloud spend**

# Effective cost management

Ownership

Frequency  
and Limits

Context and  
Response

# Set your Budgets

Scope

Total value

Thresholds

Alert levels

Integrations

Automation



**Review your Cloud spend**

Don't start  
with your invoice

# Demo – Cost Analysis





**Go fast, but go safely**



Follow my team:  
@ITOpsTalk  
[ITOpsTalk.com](http://ITOpsTalk.com) -  
Blog

@SoniaCuff  
Sonia.Cuff@microsoft.c  
om