Cloud Governance:
Winning the battle between speed & control

Sonia Cuff
Senior Cloud Advocate Microsoft
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 Admin
Replace them with a machine!
Replace them with a machine!

Developers

Operations

Built-in controls through Policy instead of workflow

Cloud custodian team
What goes into the machine?
Microsoft Cloud Adoption Framework – aka.ms/CAF

Define Strategy
- Understand motivations
- Business outcomes
- Business justification
- Prioritize project

Plan
- Digital estate
- Initial organization alignment
- Skills readiness plan
- Cloud adoption plan

Ready
- Azure readiness guide
- First landing zone
- Expand the blueprint
- Best practice validation

Adopt
- First workload migration
- Expanded scenarios
- Best practice validation

Innovate
- Innovation guide
- Expanded scenarios
- Best practice validation
- Process improvements

Govern
- Methodology
- Benchmark initial best practice
- Governance maturity

Manage
- Business commitments
- Operations baseline
- Ops maturity
What is Governance anyway?
Governance = Risk Management
Governance = Appropriate Safety Guardrails
Appropriate
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

- Cost Control
- Access to data
- Identity Security
- Access to Cloud resources
- Infrastructure Security
- Resource Consistency
- Ease of use
- Endpoint Security
- Shadow I.T.
- Availability
- Regulatory Compliance
- Guest/External Access
- Compatibility
- Complexity
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 identities and roles.
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 policies are consistent across all environments
Baseline policies

Ensure deployment consistency

App data risks

Enforce tag structure

App access risks

Design decision impact on costs
Customer scenario
Retail store applications

Production

MissionCritical
- 90210P-App1-RG
- 48015P-App2-RG

ProtectedData
- 90210P-PDApp1-RG
- 48015P-PDApp2-RG

ProdShared
- 90210P-Shared1-RG
- 48015P-Shared2-RG

OtherProd
- RSP-HR-RG
- RSP-OSHA-RG

Test

Test-Critical
- 90210T-App1-RG
- 48015T-App2-RG

Test-Protected
- 90210T-PDApp1-RG
- 48015T-PDApp2-RG

Test-Shared
- 90210T-Shared1-RG
- 48015T-Shared2-RG

Test-Other
- RST-HR-RG
- RST-OSHA-RG
Role Based Access Control
Cost Management
Cloud

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
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